Quidview Device Manager

User Manual Volume II

Hangzhou H3C Technologies Co., Ltd.

http://www.h3c.com

Manual Version: T2-08016K-20070420-C-3.13

Product Version: V3.10

Copyright © 2004-2007, Hangzhou H3C Technologies Co., Ltd. and its licensors

All Rights Reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Hangzhou H3C Technologies Co., Ltd.

Trademarks

H3C, H3C, Aolynk, Aolynk, H^{3}Care, Hcare, TOP G, TOPG, IRF, NetPilot, Neocean, NeoVTL, SecPro, SecPoint, SecEngine, SecPath, Comware, Secware, Storware, NQA, VVG, V^{2}G, V^{n}G, PSPT, XGbus, N-Bus, TiGem, InnoVision and HUASAN are trademarks of Hangzhou H3C Technologies Co., Ltd.

All other trademarks that may be mentioned in this manual are the property of their respective owners.

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

To obtain the latest information, please access:

http://www. h3c.com

Technical Support

customer_service@h3c.com

http://www. h3c.com

About This Manual

Related Documentation

Manual	Description
Quidview Device Manager User Manual Volume I	The manual provides a description of management functions of Quidview Device Manager common to routers and switches, and those specific to routers.

Organization

Quidview Device Manager User Manual Volume II s organized as follows:

Chapter	Contents
1 Overview	Gives a brief introduction to the purpose of this manual.
2 DHCP and Address Binding Management	Explains how to browse and configure the device-related information.
3 Port Management	Introduces port configuration and management functions of Quidview Device Manager.
4 VLAN Configuration	Introduces VLAN configuration and management functions of Quidview Device Manager.
5 Protocol Management	Introduces L2 protocol configuration functions of Quidview Device Manager.
6 EPON Management	Introduces EPON configuration and management functions of Quidview Device Manager.
7 VDSL Management	Introduces VDSL configuration and management functions of Quidview Device Manager.
8 Cluster Management	Introduces cluster configuration and management functions of Quidview Device Manager.
9 Stack Management	Introduces stack configuration and management functions of Quidview Device Manager.
10 QoS Management	Introduces QoS management functions of Quidview Device Manager.

Chapter	Contents
11 WLAN Management	Introduces WLAN management functions of Quidview Device Manager.
12 SMON Management	Introduces SMON management functions of Quidview Device Manager.
13 RPR Management	Introduces RPR management functions of Quidview Device Manager.
14 Auxiliary Functions	Introduces address searching and port loopback test functions of Quidview Device Manager.
15 Appendix A Abbreviations	Lists the abbreviations covered in the document and gives brief descriptions.
16 Appendix B FAQ	Lists the frequently asked questions in using Quidview Device Manager and gives solutions.
17 Appendix C Quidview License Application Procedure	Introduces how to apply for a license.

Conventions

The manual uses the following conventions:

I. GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

II. Symbols

Convention	Description
⚠ Caution	Means reader be careful. Improper operation may cause data loss or damage to equipment.
🕮 Note	Means a complementary description.

Table of Contents

Chapter 1 Overview 1-1

Chapter 2 DHCP and Address Binding Management 2-1

2.1 DHCP Management 2-1

2.1.1 DHCP Server Group 2-2

2.1.2 DHCP Relay Feature 2-3

2.1.3 DHCP Client 2-5

2.2 Address Binding Management 2-6

2.2.1 MAC-port Binding Management 2-7

2.2.2 Configuring Global MAC Address Learning 2-8

2.2.3 Configuring Port MAC Address Learning 2-9

Chapter 3 Port Management 3-1

3.1 Browsing a Port 3-1

3.2 Configuring a Port 3-3

3.3 Port MAC Mapper 3-3

3.4 Port Aggregation 3-4

3.4.1 Creating a Port Aggregation 3-5

3.4.2 Deleting a Port Aggregation 3-7

3.5 Link Aggregation Configuration 3-7

3.5.1 Adding Link Aggregation 3-7

3.5.2 Deleting Link Aggregation 3-9

3.5.3 Configuring an Aggregation Group 3-10

3.5.4 Browsing Aggregation Group Advanced Property 3-10

3.5.5 Configuring Actor Port Priority 3-10

3.5.6 Monitoring Link Aggregation 3-10

3.6 PoE Management 3-11

3.7 Transceiver Browsing 3-12

3.8 Port Isolation 3-13

Chapter 4 VLAN Configuration 4-1

4.1 Overview 4-1

4.2 VLAN Management 4-1

4.2.1 Adding a Layer 2 VLAN 4-1

4.2.2 Configuring a Layer 2 VLAN 4-3

4.2.3 Layer 2 VLAN Report 4-4

4.2.4 Deleting a Layer 2 VLAN 4-4

4.3 VLAN Interface Management 4-4

4.3.1 Adding a VLAN Interface 4-4

4.3.2 Configuring a VLAN Interface 4-5

4.3.3 VLAN Interface Report 4-6
4.3.4 Deleting a VLAN Interface 4-6
4.4 VLAN Trunk Management 4-6
4.4.1 Adding a VLAN Trunk 4-6
4.4.2 Configuring a VLAN Trunk 4-8
4.4.3 VLAN Trunk Report 4-8
4.4.4 Deleting a VLAN Trunk 4-8
4.5 VLAN Hybrid Management 4-8
4.5.1 Adding a VLAN Hybrid Port 4-8
4.5.2 Configuring a VLAN Hybrid Port 4-10
4.5.3 VLAN Hybrid Report 4-10
4.5.4 Deleting a VLAN Hybrid Port 4-10
4.6 Isolate-VLAN Management 4-10
4.6.1 Introduction to Isolate-VLAN 4-10
4.6.2 Adding an Isolate-VLAN 4-11
4.6.3 Configuring an Isolate-VLAN 4-11
4.6.4 Deleting an Isolate-VLAN 4-11
4.7 Adding a Port to VLAN 4-11
4.8 Protocol VLAN Management 4-12
4.8.1 Adding a Protocol VLAN 4-12
4.8.2 Configuring a Protocol VLAN 4-14
4.9 Voice VLAN Management 4-15
4.9.1 Configuring Voice VLAN Ports 4-16
4.9.2 OUI Configuration 4-17

Chapter 5 Protocol Management 5-1
5.1 Overview 5-1
5.1.1 STP/RSTP 5-1
5.1.2 GARP 5-1
5.1.3 GVRP 5-2
5.1.4 GMRP 5-2
5.1.5 IGMP Snooping 5-3
5.1.6 MSTP 5-3
5.2 Configuring the RSTP 5-4
5.2.1 Configuring the RSTP of a Device 5-4
5.2.2 Configuring Port RSTP 5-6
5.3 Configuring the GARP 5-8
5.3.1 Configuring Global GARP 5-8
5.3.2 Configuring Port GARP 5-9
5.4 Configuring the IGMP Snooping 5-10
5.5 MSTP Protocol Configuration 5-11
5.5.1 MSTP Protocol Configuration 5-11
5.5.2 MSTI Protocol Configuration 5-14

5.5.3 Port MSTP Protocol Configuration 5-16

Chapter 6 EPON Management 6-1

6.1 Overview 6-1
6.2 EPON System Management 6-3
6.3 EPON OLT Management 6-5
6.3.1 OLT System Information 6-5
6.3.2 DBA Algorithm Management 6-7
6.3.3 OLT Primary Status 6-9
6.3.4 OLT Alarm Configuration 6-9
6.4 EPON ONU Management 6-12
6.4.1 ONU System Information 6-12
6.4.2 Link Test Management 6-13
6.4.3 Downstream Bandwidth Management 6-14
6.4.4 ONU MAC Address Configuration 6-15
6.4.5 Upstream Bandwidth Management 6-15
6.4.6 ONU Primary Status 6-16
6.4.7 ONU Software Update 6-16
6.4.8 ONU Packet Management 6-16
6.4.9 ONU Protocol Management 6-17
6.4.10 ONU dot1x Authentication 6-18
6.5 EPON Batch Operation 6-18
6.5.1 Batch Operation by Slot 6-19
6.5.2 Batch Operation by OLT 6-19
6.6 EPON OAM Management 6-20
6.6.1 EPON OAM Configuration 6-20
6.6.2 EPON OAM Peer Information Browsing 6-20
6.6.3 EPON OAM Loop Back 6-20
6.6.4 EPON OAM Event Configuration 6-21
6.6.5 EPON OAM Event Log 6-21
6.6.6 EPON OAM Statistic 6-21
6.7 EPON Device Management 6-21
6.7.1 EPON Device Control 6-22
6.7.2 EPON MAC Address LLID of ONU 6-23
6.7.3 EPON Device Statistic 6-23
6.8 EPON UNI Management 6-23
6.8.1 UNI Port Management 6-24
6.8.2 UNI Port Traffic Statistics 6-26
6.8.3 UNI Port Multicast Information 6-26

Chapter 7 VDSL Management 7-1

7.1 Overview 7-1
7.2 VDSL Port Configuration 7-1
7.2.1 Browsing Port Link Data 7-1

7.2.2 Browsing Port Version Information 7-2
7.2.3 Port Template Management 7-3
7.2.4 Port Parameter Configuration 7-4
7.3 VDSL Port Performance Monitoring 7-6

Chapter 8 Cluster Management 8-1
8.1 Overview 8-1
8.1.1 Concept of Cluster 8-1
8.1.2 Features of Cluster 8-3
8.1.3 Cluster Management of Quidview Device Manager 8-3
8.2 V1 Cluster Management 8-5
8.2.1 Cluster Creation and Maintenance 8-5
8.2.2 Client Switch Management 8-6
8.2.3 Other Functions 8-13
8.3 V2 Cluster Management 8-13
8.3.1 Cluster Creation and Maintenance 8-13
8.3.2 Other Functions 8-18

Chapter 9 Stack Management 9-1
9.1 Overview 9-1
9.1.1 Concept and Features of Stack 9-1
9.1.2 Stack Management of Quidview Device Manager 9-1
9.2 Managing and Maintaining the Stack 9-2
9.2.1 Creating a Stack 9-2
9.2.2 Opening a Stack 9-2
9.2.3 Configuring Stack Protocols 9-3
9.2.4 Configuring Stack VLAN 9-4
9.2.5 Browsing and Configuring Stack Port 9-4
9.2.6 Stack Member List 9-4
9.2.7 Identifying Stack Port 9-5
9.2.8 Deleting a Stack 9-5

Chapter 10 QoS Management 10-1
10.1 QoS Overview 10-1
10.1.1 ACL 10-1
10.1.2 What is QoS 10-1
10.1.3 QoS of Quidview Device Manager 10-2
10.2 Time-Range Configuration 10-3
10.2.1 Adding a Time-Range 10-3
10.2.2 Deleting a Time Range 10-6
10.3 ACL Configuration 10-6
10.3.1 Adding a Standard ACL 10-7
10.3.2 Adding an Extended ACL 10-8
10.3.3 Adding a Layer-2 ACL 10-9

10.3.4 Deleting an ACL 10-10
10.4 QoS Configuration 10-10
10.4.1 Traffic Limit 10-10
10.4.2 Traffic Priority 10-12
10.4.3 Traffic Redirect 10-12
10.4.4 Traffic Statistics 10-13
10.4.5 Mirrored To 10-13
10.4.6 Packet Filtering 10-13
10.4.7 Configuring and Deleting QoS Items 10-14
10.5 QoS Properties 10-14
10.5.1 Port Queue Schedule 10-16
10.5.2 WRED Parameters 10-17
10.5.3 Port Drop Mode 10-19
10.5.4 Service Parameters 10-20

Chapter 11 WLAN Management 11-1
11.1 Overview 11-1
11.2 Configuration Parameters Management 11-1
11.2.1 System Attributes Management 11-1
11.2.2 System Configuration Management 11-2
11.3 Site Configuration Management 11-3
11.3.1 Information Management 11-3
11.3.2 Wireless Interface Management 11-4
11.3.3 Station Management 11-5
11.3.4 Filter Management 11-6
11.3.5 Connection Information 11-8
11.3.6 Authentication Management 11-8
11.3.7 Anonymous SSID Management 11-10
11.4 Physical Layer Management 11-11
11.4.1 Antenna Management 11-11
11.4.2 Transmit Power Management 11-13
11.4.3 Antenna List Management 11-14
11.5 Encryption Management 11-15
11.5.1 Encryption Table Management 11-15
11.5.2 Default Key Table Management 11-17
11.6 Performance Statistics 11-18
11.6.1 Wireless Interface 11-19
11.6.2 WLAN Terminal User 11-19
11.6.3 Access Request Reject Reason 11-19
11.6.4 Reason for Detachment and Authentication Cancel 11-19
11.6.5 MAC Address 11-19
11.6.6 User Info. In AP Initialization 11-20
11.6.7 EAP-SIM Authentication between AP and AS 11-20

11.6.8 EAP-SIM Authentication between AAPP and All WLAN Terminal Users..... 11-20
11.6.9 EAP-SIM Authentication between AP and Individual WLAN Terminal User..... 11-20

Chapter 12 SMON Management 12-1
12.1 SMON Data Source Management 12-1
12.2 VLAN Statistics Management 12-2
12.3 VLAN Priority Statistics Management 12-6
12.4 VLAN Static Statistics Management 12-9

Chapter 13 RPR Management 13-1
13.1 Logical and Physical Interfaces of RPR 13-1
13.2 RPR Interface Management 13-2
13.3 Statistic Data Management 13-4
13.4 Protection Parameters Configuration 13-5
13.5 Fairness Management 13-7
13.6 OAM Management 13-8
13.7 Span Browsing 13-10
13.8 TOPO Ring Browsing 13-10
13.9 RPR Real time Monitor 13-11

Chapter 14 Auxiliary Functions 14-1
14.1 Address Searching 14-1
14.2 Port Loopback Test 14-4

Chapter 1 Overview

This manual serves as a companion to *Quidview Device Manager User Manual Volume I*. It is designed to introduce the management provided by Quidview Device Manager for H3C (Hangzhou H3C Technologies Co., Ltd.) Series Ethernet switches and WLAN Series products and specially intended to introduce some Ethernet switch and WLAN product specific features like port, VLAN, protocol, EPON, VDSL, cluster, stack, and QoS management. The detail on the general functionalities and topology management of Quidview Device Manager is elaborated in Volume I and so is omitted here.

Chapter 2 DHCP and Address Binding Management

This chapter mainly introduces the DHCP management and address binding management functions of Device Manager on switches.

Address binding is a simple security mechanism and the base of implementing some advanced security protocols. H3C switch products support the following address binding modes:

- MAC-port binding: It limits the port of a host (PC or network device) with a specified MAC address must be connected to in order to use network resources.
- IP-MAC binding: It allows you to add the corresponding relation between an IP address and a MAC address to a switch to ensure the network access authority of a legal user with fixed IP address and to prohibit hosts with illegal IP addresses from accessing network resources.
- IP-MAC-port binding: It allows you to bind the corresponding relation between an IP address and a MAC address to a specified port through static ARP so that the host with the IP and MAC addresses can access the network only when being connected to the specified port. This prevents IP address embezzlement and limits the port over which a host can communicate with outside on physical layer.

At present, the first two address binding modes can be configured in the NMS. IP-MAC binding is implemented over DHCP-Relay. This feature is covered in section 2.1 “DHCP Management”. MAC-port binding will be introduced in section 2.2 “Address Binding Management”.

2.1 DHCP Management

In the function window, double-click on the [Device management/DHCP management] node to open the [DHCP Management] dialog box. This interface includes DHCP server group information, DHCP relay feature and DHCP client information, as shown in Figure 2-1.

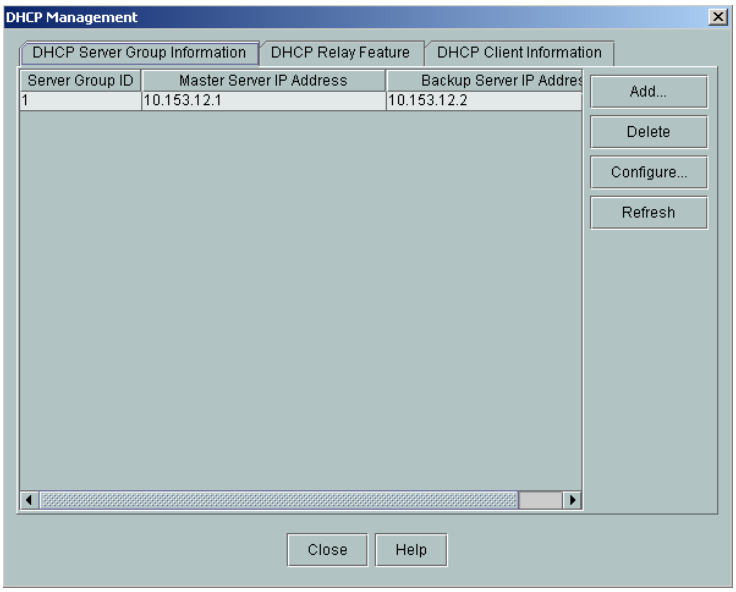


Figure 2-1 DHCP management (DHCP server group information)

2.1.1 DHCP Server Group

As shown in Figure 2-1, the [DHCP Server Group Information] tab displays the DHCP server information configured on the device, including server group ID, master server IP address and backup server IP address.

I. Adding a DHCP group

In Figure 2-1, click <Add…> to open the [Add DHCP Server Group] dialog box, as shown in Figure 2-2.

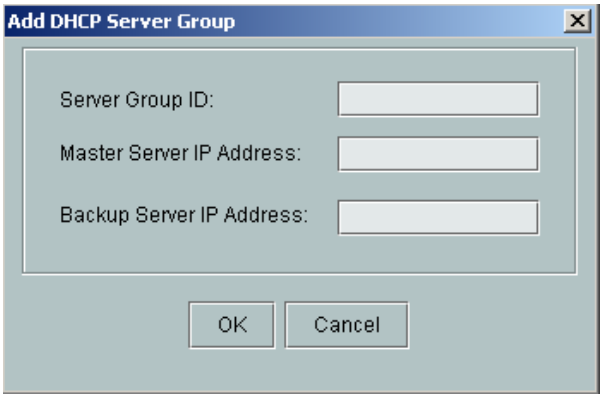


Figure 2-2 Adding a DHCP server group

The information required in the interface is described in the following table:

Table 2-1 Information required in adding a DHCP server group

Parameter name	Parameter description
Server group ID	It ranges from 0 to 19
Master server IP address	It is a valid IP address and belongs to a single group, that is, you cannot create several groups for a master DHCP server.
Backup server IP address	A valid IP address

To improve reliability, you can configure a master and a backup DHCP server for a network segment to build up a DHCP server group.

II. Deleting a DHCP group

In Figure 2-1, select one or more DHCP server groups and click <Delete> to delete them.

III. Modifying a DHCP group

In Figure 2-1, select a DHCP server group to be modified and click <Configure…> to open the dialog box shown in Figure 2-2. Here modify the IP address of the master or (and) backup DHCP server and click <OK> to confirm your modification.

IV. Refreshing DHCP group information

In Figure 2-1, click <Refresh> to refresh the DHCP server group information of the device.

2.1.2 DHCP Relay Feature

In Figure 2-1, click the [DHCP Relay Feature] tab to switch to the corresponding page that shows such information as VLAN interface, server group ID and DHCP address check. Here you can configure the DHCP server group corresponding to a VLAN interface, as shown in Figure 2-3.

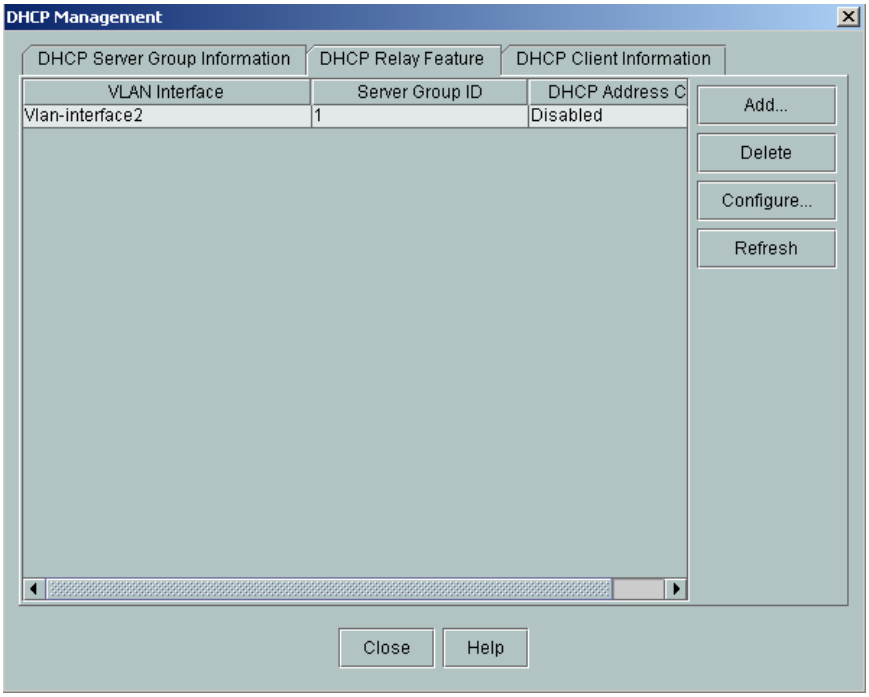


Figure 2-3 DHCP relay feature

I. Adding a DHCP relay

In Figure 2-3, click <Add…> to enter the [Add DHCP Relay Feature] dialog box, as shown in Figure 2-4.

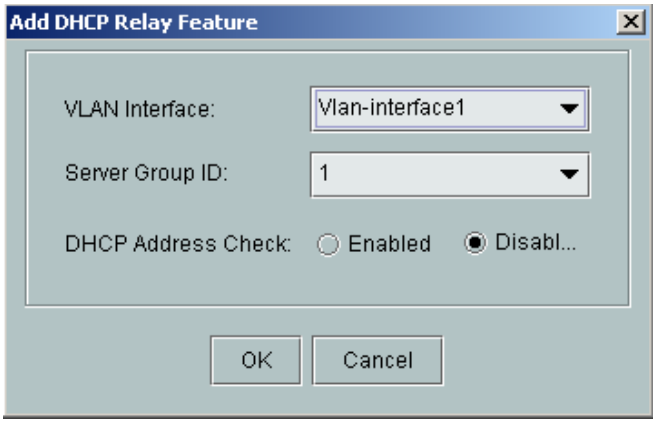


Figure 2-4 Adding DHCP relay feature

The information required in the interface is described in the following table:

Table 2-2 Information required in adding a DHCP relay feature

Parameter name	Parameter description
VLAN interface	Select a VLAN interface name from the drop-down list.
Server Group ID	Select a DHCP server group ID from the drop-down list of the created ones.

Parameter name	Parameter description
DHCP Address check	Set whether to enable DHCP address check. Selecting "Enabled" will enable the validity check for user addresses on the VLAN interface, and selecting "Disabled" will disable the check.

II. Deleting a DHCP relay

In Figure 2-3, select one or more DHCP relays and click <Delete> to delete them.

III. Modifying a DHCP relay

In Figure 2-3, select a DHCP relay and click <Configure…> to open the [Add DHCP Relay Feature] dialog box, as shown in Figure 2-4. Here modify the server group ID and the status of DHCP address check, and click <OK> to confirm your modification.

IV. Refreshing DHCP relay information

In Figure 2-3, click <Refresh> to refresh the DHCP relay information of the device.

2.1.3 DHCP Client

In Figure 2-1, click the [DHCP Client Information] tab to switch to the corresponding page that shows such information as client IP address, client MAC address and address type, as shown in Figure 2-5.

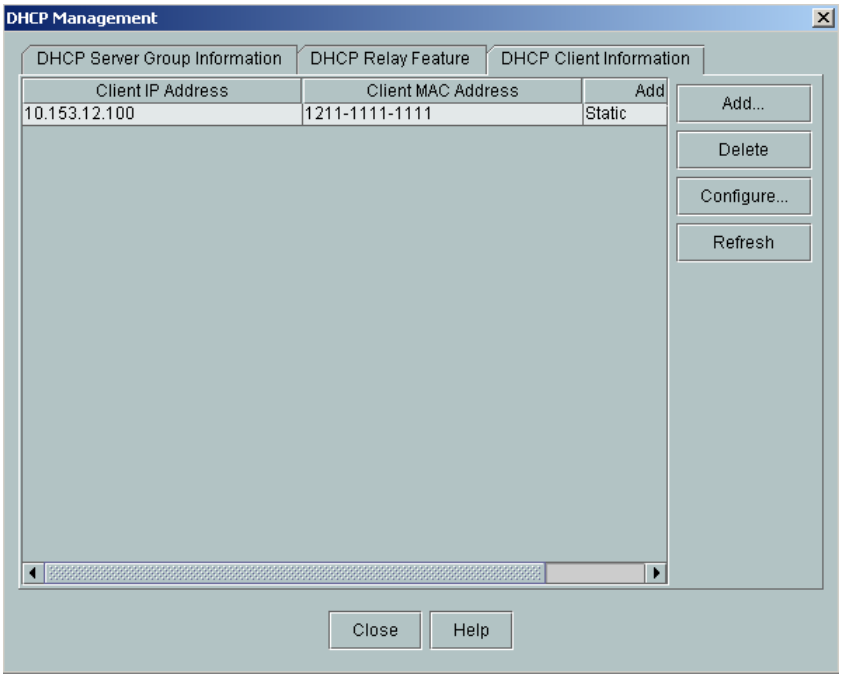


Figure 2-5 DHCP client information

I. Adding a DHCP client address

In Figure 2-5, click <Add…> to open the [Add DHCP Client Address] dialog box, as shown in Figure 2-6.

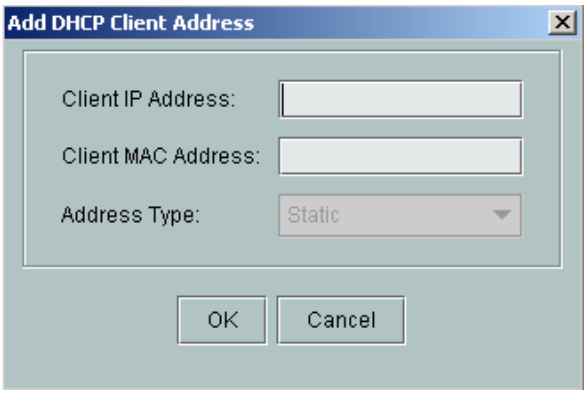


Figure 2-6 Adding a DHCP client address

In order for a legal user with fixed IP address of a VLAN configured with DHCP relay to pass the DHCP address check, you should add an entry for the user, correlating the IP address and the MAC address. If an illegal user is configured with a static IP address that conflicts with the fixed IP address of the legal user, it will be recognized by the Ethernet switch running DHCP-relay function, and be prohibited from binding its IP address and MAC address.

II. Deleting a DHCP client address

In Figure 2-5, select one or more DHCP client addresses, and click <Delete> to delete them.

III. Modifying a DHCP client address

In Figure 2-5, select a DHCP client address and click <Configure…> to open the [Add DHCP Client Address] dialog box, as shown in Figure 2-6. Here modify the DHCP client IP address, MAC address and device type, and click <OK> to confirm your modification.

IV. Refreshing DHCP client address information

In Figure 2-5, click <Refresh> to refresh the DHCP client address information of the device.

2.2 Address Binding Management

In the function window, double-click on the [Device Management/Address Binding Management] node to open the [Address Binding Management] dialog box. This interface includes three kinds of information, that is, MAC port binding management,

global MAC address learning configuration and port MAC address learning configuration, as shown in Figure 2-7.

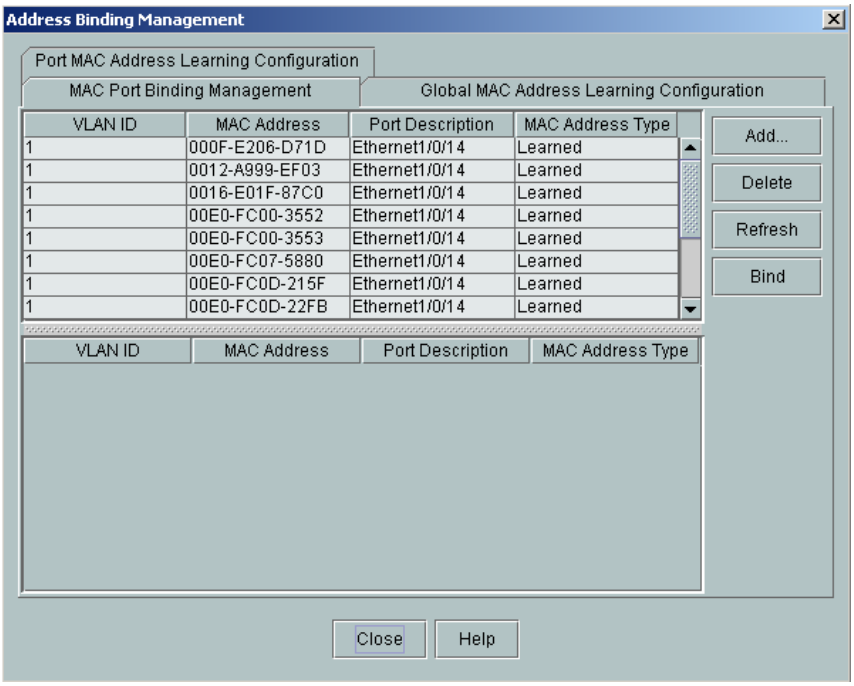


Figure 2-7 Address binding management (MAC-port binding management)

2.2.1 MAC-port Binding Management

This function limits the port to which a host (PC or network device) with a specified MAC address must be connected in order to access the network resources. As shown in Figure 2-7, the upper part displays the dynamic MAC-port binding list, and the lower part displays the static MAC-port binding list.

I. Adding a MAC-port binding

In Figure 2-7, click <Add…> to open the [Add MAC Port Binding Information] dialog box, as shown in the following figure:

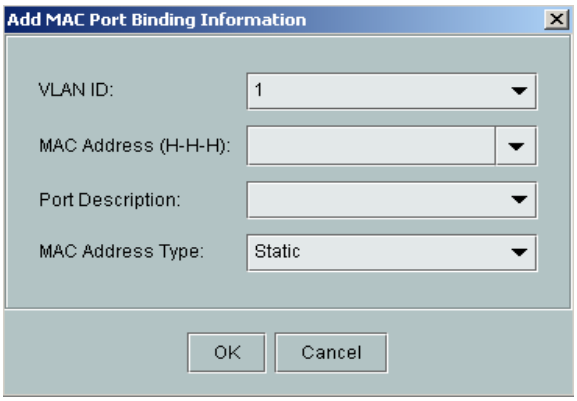


Figure 2-8 Adding MAC-port binding information

Here you can bind a VLAN port to a MAC address. The information required in the interface is described in the following table:

Table 2-3 Information required in adding MAC-port binding information

Parameter name	Parameter description
VLAN ID	Select a VLAN ID from the drop-down list
MAC address	A valid MAC address (MAC address must be multicast address, i.e., the second bit must be even.)
Port description	Select a port number from the drop-down list
MAC address type	Include static and dynamic.

II. Deleting a MAC-port binding

In Figure 2-7, select one or more MAC-port binding configurations and click <Delete> to delete them.

Note:

If you click <Refresh> right after the Mac-port binding information is deleted, the deleted information may be displayed again. This is because the device is synchronizing the software and hardware entries, and you are recommended to refresh after the synchronization completes.

III. Refreshing MAC-port binding information

In Figure 2-7, click <Refresh> to refresh the MAC-port binding information of the device.

IV. Binding

Select a row in the dynamic MAC-port binding list, and click <Bind> to make the binding become static. This row will be deleted from the dynamic MAC-port binding list, and be added to the static one.

2.2.2 Configuring Global MAC Address Learning

In Figure 2-7, click the [Global MAC Address Learning Configuration] tab to switch to the corresponding page, showing the MAC address aging time, as shown in the following figure:

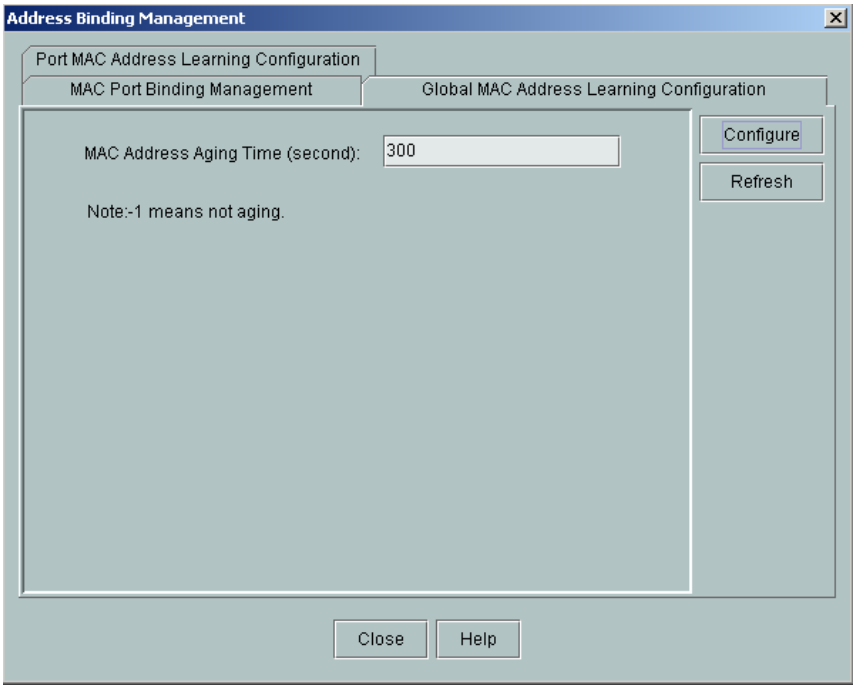


Figure 2-9 Global MAC address learning configuration

Setting a proper aging time helps implement the MAC address aging function effectively. Setting the aging time too long or too short may lead the Ethernet switch to broadcast a great amount of packets with unknown destination MAC addresses and affect the operation performance of the switch.

If the aging time is too long, the Ethernet switch may keep many outdated MAC address entries, which will use up the MAC address table resource and make it impossible for the switch to update the MAC address table according to the changes of the network. If the aging time is too short, the Ethernet switch may delete some effective MAC address entries frequently, which will cause the generation of too many ARP update messages and slow down system response.

2.2.3 Configuring Port MAC Address Learning

In Figure 2-7, click the [Port Address Learning Configuration] tab to switch to the corresponding page, showing the status of MAC address learning and the maximum number of learnable MAC addresses on each port, as shown in the following figure:

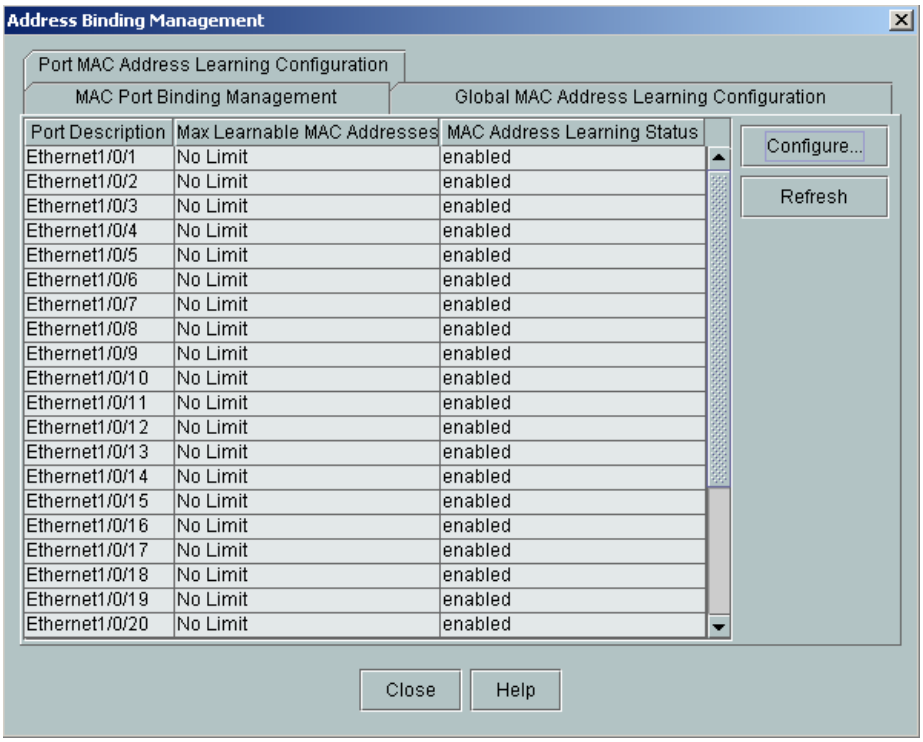


Figure 2-10 Port MAC address learning configuration

Through MAC address learning, an Ethernet switch can get the MAC addresses of various network devices on the network segment connected to certain port. With this knowledge, the Ethernet switch can directly perform hardware forwarding on the packets heading for these MAC addresses. An oversized MAC address table may reduce the forwarding performance of the Ethernet switch.

By setting the maximum number of learnable MAC addresses of an Ethernet port, you can limit the number of entries contained in a MAC address table maintained by an Ethernet switch. When the number of entries exceeds the maximum value, the port will on longer learn any MAC address.

Select a port MAC address learning configuration and click <Configure…> to modify the maximum number of learnable MAC addresses of the port.

Chapter 3 Port Management

3.1 Browsing a Port

I. Operation procedure

After the Quidview Device Manager starts, select the menu [Device/Open Device…] or click the button on the toolbar to open the panel view of the switch. Then select [Port Management/Port Browsing] node from the function window to open the [Port Browsing] dialog box, as shown in Figure 3-1.

The Port Browsing dialog box is used to browse the configuration information about the specified port. You can modify the information through clicking <Configure…> or using the method described in section 3.2 “Configuring a Port”. If none of the ports is selected, the information of all the ports will be listed.

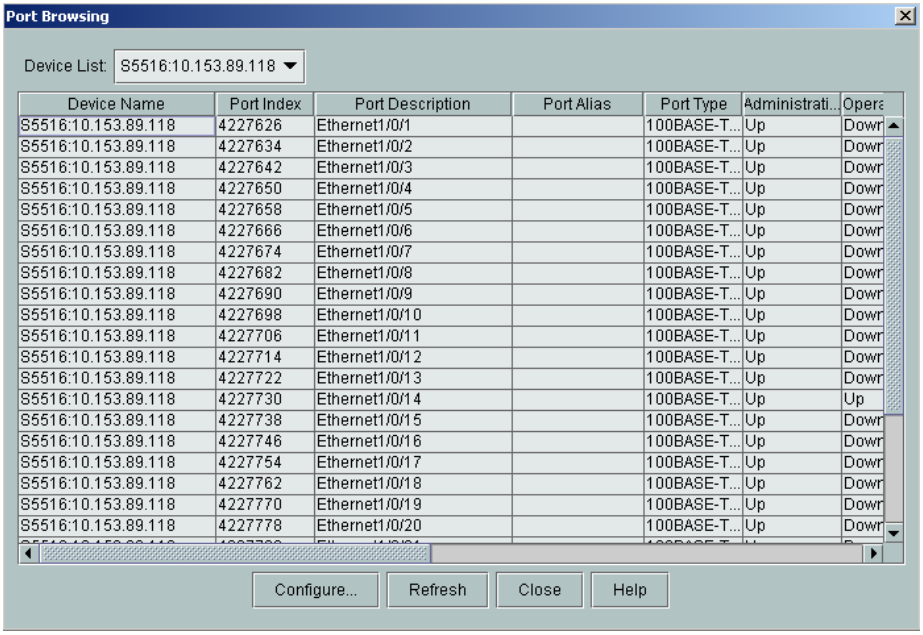


Figure 3-1 Port Browsing

II. Parameter description

1) Port Alias

It is the alias of the port, and you can configure on your demand.

2) Port Type

It is the type of the port. The fixed port on an Ethernet switch is usually an Ethernet port.

3) Administrative Status

It is the administrative status of the port, including Up and Down. It performs the function similar to the "shut" command.

4) Operation Status

It is the actual link status of the port, including Up and Down.

5) Duplex Mode

It identifies the work mode of the port, such as full-duplex, half-duplex and self-sensing.

6) Configuration Rate

It sets the rate of the Ethernet port to 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s or auto (negotiation). By default, it is "Auto".

7) Real Rate

It is the real rate such as 10 Mbps, 100 Mbps or 1000 Mbps at which the port receives and sends packets.

8) Broadcast Suppression

It sets the maximum broadcast traffic through the Ethernet port. When the broadcast traffic crosses certain threshold, the system will drop the follow on traffic to ensure the normal services on the network and to limit the percentage of broadcast traffic to a reasonable range. This parameter tasks the percentage of the maximum broadcast traffic line rate through the port. The smaller the percentage is, the smaller the allowed broadcast traffic. When the percentage is set to 100, broadcast storm restrain is disabled on the port.

9) Flow Control Status

It sets whether to control the traffic through the Ethernet port, where "True" indicates to control and "False" indicates not to control.

10) Default User Priority

It is the packet tag priority. When it is set to 0, the priority of the packets passing through will not be modified.

11) PVID

It is the PVID of the port. By default, a port is configured with a PVID.

12) VLAN Port Type

It sets the VLAN port type of the port, including Access, Trunk and Hybrid. "Access" refers to a normal port, that is, a port belonging to a single VLAN. "Trunk" refers to a Trunk port through which packets from several tagged VLANs can pass. A "Hybrid" port combines the attributes of an "Access" port and a "Trunk" port, and can forward untagged VLANs' packets.

13) Aggregation Status

Identify whether a port joins port aggregation. If yes, whether it is aggregated to the master port or the sub-port is displayed.

3.2 Configuring a Port

Select a port, and select [Port Management/Port Configuration] from the function window to open the [Port Configuration] dialog box, as shown in Figure 3-2. The parameter description is covered in section 3.1 “Browsing a Port”.

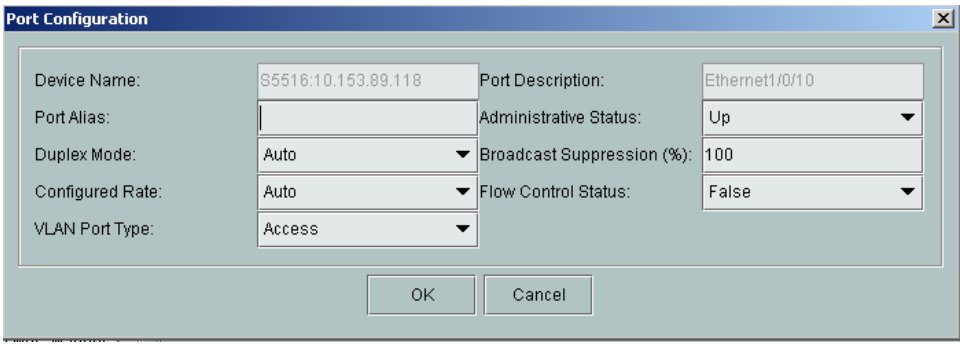


Figure 3-2 Port Configuration

3.3 Port MAC Mapper

Click "+" on the [Port Management] node in the function window, then double-click the extended leaf node [Port MAC Mapper], and the [Port MAC Mapper] dialog box will pop up, as shown in Figure 3-3.

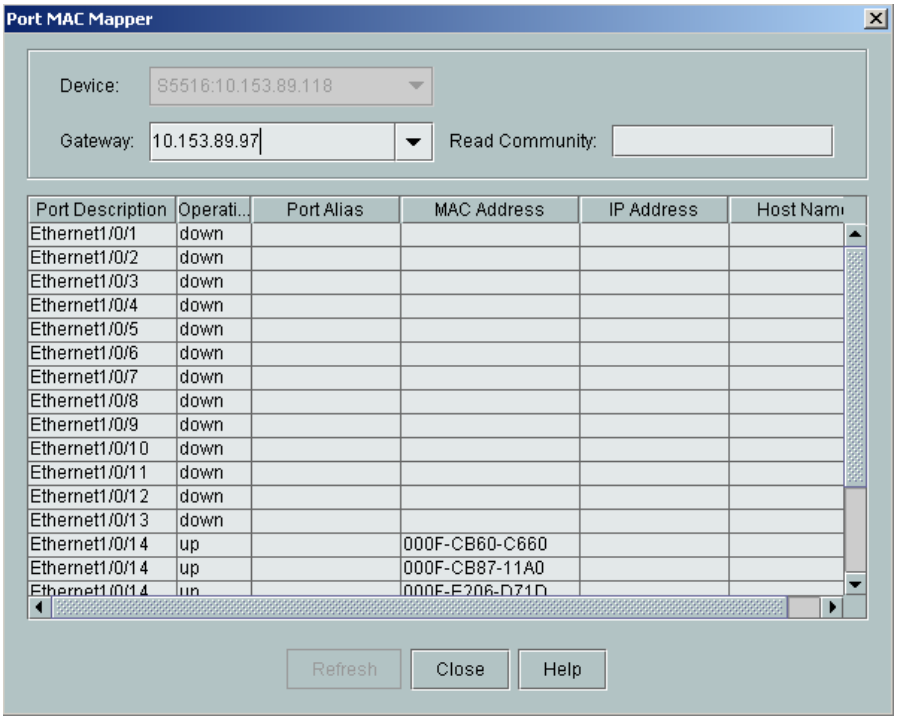


Figure 3-3 Port MAC Mapper

The dialog box displays switch ports and some information about their connected devices, including port description, operation status, port alias, and MAC addresses, IP addresses and host names of the devices connected on the ports.

The "Gateway" displays the default gateway in the routing table of the switch. The system treats it as a default gateway to obtain information about the devices connected on the ports. You can alternatively input a gateway here. If what you input is inaccessible, the system adopts the default gateway.

The "Read Community" defaults to "public". You can also input a community name to access the gateway you defined.

3.4 Port Aggregation

Note:

The port aggregation menu may vary, depending on which version of software is installed on device. This section and section 3.5 “Link Aggregation Configuration” both introduce link aggregation function, but it may have a different menu depending on the version of software installed.

Port aggregation means to aggregate multiple ports so that member ports can share the outgoing/incoming loads. From the outside, an aggregation group looks like one port.

The Ethernet switches support different number of port aggregation groups and maximum number of ports in each aggregation group. For the specific differences, refer to related device manuals.

Note:

- When the S3526 has several aggregation groups, the same aggregation mode must be used for every group.
- The S6506 ports to be aggregated must be located on the same board. For the gigabyte electrical and optical interface boards, up to 8 ports can be aggregated. For the 100M electrical interface board, the number is 24.
- The ports contained in each S3026V aggregation group must be of the same type.

3.4.1 Creating a Port Aggregation

Click "+" on the [Port Management] node in the function window, then double-click the extended leaf node [Port Aggregation] to open the [Port Aggregation] dialog box, as shown in Figure 3-4.

The [Port Aggregation] dialog box is the main interface for implementing port aggregation management. This dialog box displays the number of aggregated ports and the basic information on the device. Clicking the buttons at the bottom of the interface, the user can create new port aggregation, refresh the port aggregation information about the device or delete the existing port aggregation.

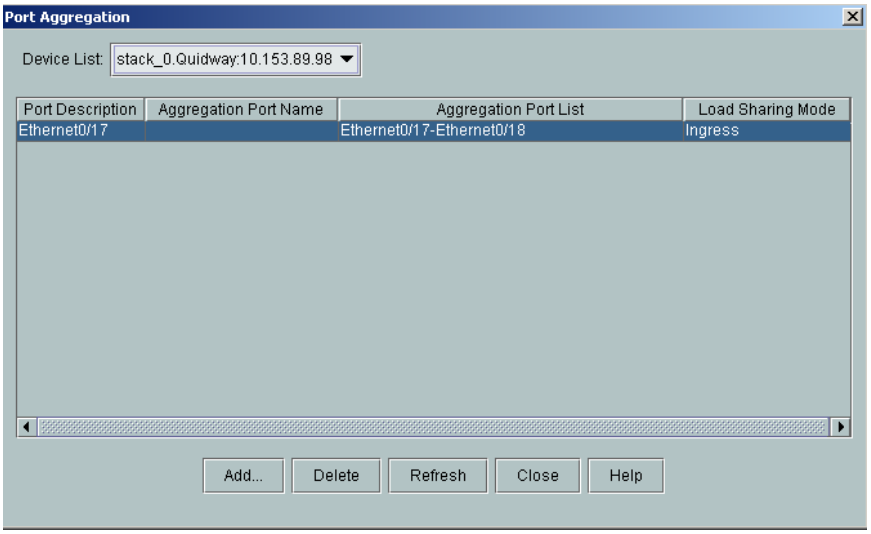


Figure 3-4 Port Aggregation

Click <Add…> on the interface to pop up the [Add Port Aggregation] dialog box, as shown in Figure 3-5.

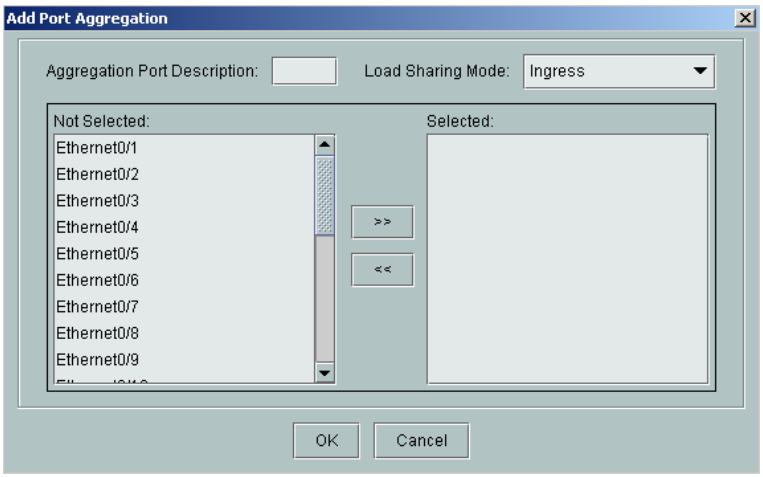


Figure 3-5 Adding port aggregation

Users should first select a group of ports used for aggregation in the left of the device port list. Click to add these ports to the selected ports List. Then enter the name of the port aggregation in the editing column of the [Aggregation Port Description] field and select a load-sharing mode in the drop-down list. Click <OK> to add a port aggregation.

The load-sharing mode has the following options:

- Ingress: Indicates that the member ports in the aggregation group share the loads of outgoing data traffic only according to the source MAC address.
- Both: Indicates that the member ports in the aggregation group share the loads of outgoing data traffic according to the source MAC address and destination MAC address.
- Round_robin: Indicates that the member ports in the aggregation group share the loads of outgoing data traffic according to the metric values of the aggregated ports.

🕮 **Note:**

- Observing port and ports already involved in other link-aggregations are not available for new aggregations. So they will not appear in the [Master Port] list. What's more, auto-negotiating port cannot be used in aggregations;.
- After selecting the master port, contents in the Available Port List will change respectively. All the slave ports involved in a link-aggregation cannot exceed the number of 7.

3.4.2 Deleting a Port Aggregation

Select an aggregation port to be deleted in the [Port Aggregation] dialog box shown in Figure 3-4. Click <Delete> to delete the specified port aggregation after confirmation.

3.5 Link Aggregation Configuration

🕮 **Note:**

The port aggregation menu may vary, depending on which version of software is installed on device. This section and section 3.4 “Port Aggregation” both introduce link aggregation function, but it may have a different menu depending on the version of software installed.

Link aggregation bundles together multiple links on a device, to broaden bandwidth and improve reliability of the links. The aggregated links can be treated as one link externally.

The IEEE802.3ad-compliant LACP (Link Aggregation Control Protocol) is a protocol used for dynamic link aggregation and deaggregation. It presents immediate adaptability to distributed aggregated links, accommodating momentary network topology changes. LACP provides a standard means, by which the local (Actor) and the peer (Partner) exchange information through links and reach consensus on the joined or quitted aggregation group of the links.

3.5.1 Adding Link Aggregation

In the function window, click "+" on the "Port Management" node, then double-click the extended leaf node "Port Aggregation” and the [Port Aggregation] dialog box will pop up, as shown in Figure 3-6.

The [Port Aggregation] dialog box is a main interface for link aggregation management. It displays quantity of link aggregation and relevant information. You can create, refresh or delete link aggregation by clicking different buttons at the bottom of the interface.

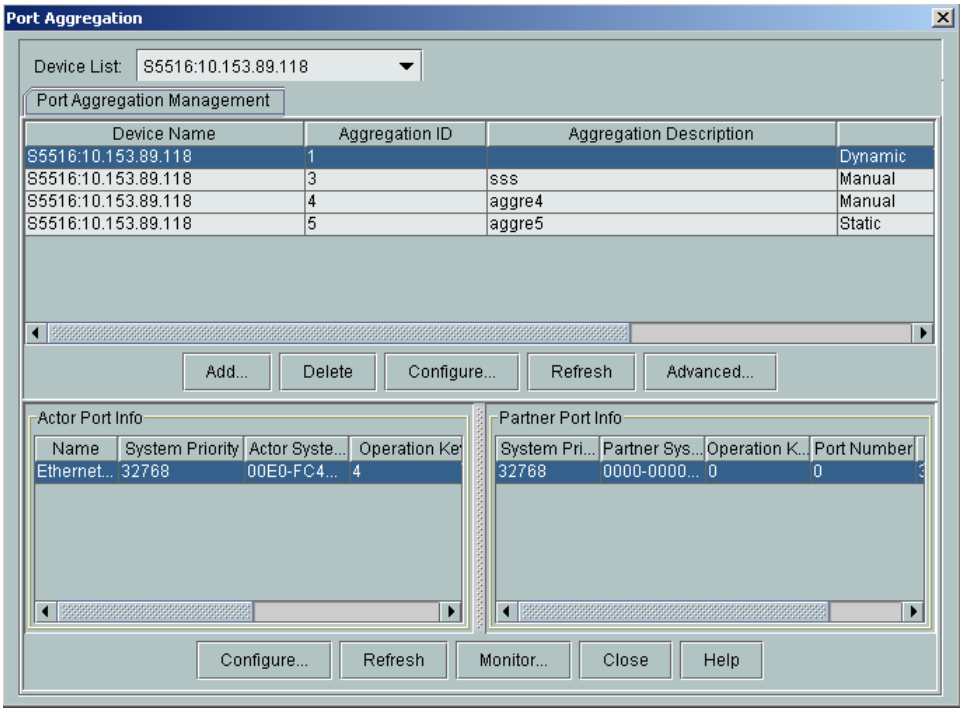


Figure 3-6 Port Aggregation

Click <Add…>, and then the [Create Aggregation (1)] dialog box will pop up. Input a valid aggregation ID and click <Next>, and the [Create Aggregation] dialog box will pop up, as shown in Figure 3-7.

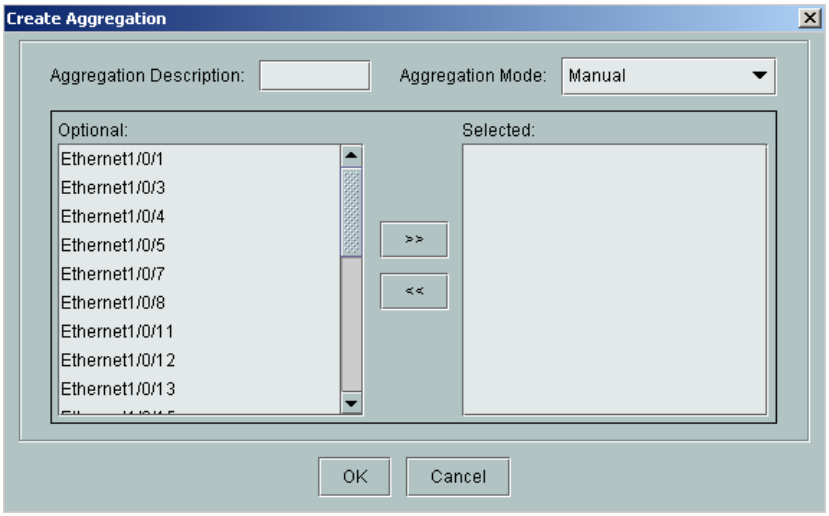


Figure 3-7 Create Aggregation

Select a group of aggregation ports in the left Optional field, and then click to add these ports into the selected aggregation ports list. In the [Aggregation Description] text box, input the name of the aggregation group. In the Aggregation Mode list box, select an aggregation mode. Click <OK> and you can create a new link aggregation group.

Optional aggregation modes include:

- Manual: Manual aggregation is a group of manually configured aggregation ports, which the system cannot automatically add or delete. LACP is disabled for manual aggregation ports. You are not permitted to enable it.
- Static: Like manual aggregation, static aggregation is also a group of manually configured aggregation ports, which the system cannot automatically add or delete. Different from manual aggregation, however, LACP must be enabled here. When a static aggregation group is deleted, its member ports form one or more dynamic LACP aggregations, with LACP enabled. You are not permitted to disable LACP for static aggregation ports.
- Dynamic: Dynamic aggregation is automatically created/deleted by the system. You are not permitted to add or delete member ports in dynamic LACP aggregation.

Note:

- Observation ports and aggregation ports cannot be used for other link aggregation any more; therefore, they are not included in the drop-down list describing the main port. Besides, auto-negotiation ports cannot act as aggregation ports either.
- After you select a main port, optional ports listed in the left of the interface may automatically change. One link aggregation cannot contain more than seven member ports.

3.5.2 Deleting Link Aggregation

In the [Port Aggregation] dialog box, select an aggregation group to be deleted and click <Delete>, and then the specified link aggregation is deleted.

You can delete any existing aggregation group on a device. If you delete a manual/dynamic aggregation group, all ports in the aggregation group will leave the group; if you otherwise delete a static aggregation group, ports of the aggregation group will form one or more dynamic aggregation groups.

According to LACP, when you delete a dynamic aggregation group, another aggregation group will be automatically created (possibly with a different aggregation group ID). If you want to terminate this automatic creation process, you must disable all

ports in the dynamic aggregation group. When you delete a dynamic aggregation group, the Quidview system reckons that you mean to terminate the automatic creation of another dynamic aggregation group.

3.5.3 Configuring an Aggregation Group

In the [Port Aggregation] dialog box, select a dynamic or static aggregation group you want to configure and click <Configure…>, then the [Port Aggregation Management] dialog box will pop up. In the dialog box, you can configure a name for a static aggregation group and its optional ports. As for a dynamic aggregation group, you can only configure its name but not its ports.

3.5.4 Browsing Aggregation Group Advanced Property

For the aggregation groups with the aggregation mode as static or dynamic, you can view their advanced properties. In the [Port Aggregation] dialog box shown in Figure 3-6, select an aggregation group you want to browse and click <Advanced…>, and then the [Aggregation Advanced Property] dialog box will pop up. This dialog box shows some properties about the aggregation group, including its MAC address, aggregated or not, actor system priority, actor system ID, actor operation key, partner system priority, partner system ID, and partner operation key.

You can configure the actor system priority in this dialog box, and then click <OK> to complete the configuration.

3.5.5 Configuring Actor Port Priority

In the [Port Aggregation] dialog box shown in Figure 3-6, select a static or dynamic aggregation group, and then the lower part of the dialog box will display some general information about the actor port and the partner port. In the [Actor Port Info] section, select a port you want to configure and click <Configure…>, then the [Aggregation Port Configuration] dialog box will pop up, you can configure the priority of the port in the dialog box and click <OK> to complete the configuration.

3.5.6 Monitoring Link Aggregation

In the [Port Aggregation] dialog box shown in Figure 3-6, select a static or dynamic aggregation group, and then the lower part of the dialog box will display some general information about the actor port and the partner port. In the [Actor Port Info] section, select a port you want to monitor and click <Monitor…>, and then the [Port Traffic Monitoring] dialog box will pop up for you to monitor the traffic on the port in real time.

3.6 PoE Management

Power over Ethernet (POE) technology allows IP phones, WLAN access point and other devices to receive power as well as data over the existing LAN cabling, without modification to the existing Ethernet architecture. It has become an international standard, called IEEE802.3af, as an extension to the existing Ethernet standards.

Specific to PoE devices, Quidview Device Manager supports browsing and querying power supply configuration and state. PoE interface browse enables user to browse the power parameters of power supply sets and interfaces on PoE devices, and PoE interface configuration to set or modify these parameters for the demands on application.

The description on the main parameters is shown in Table 3-1 and Table 3-2.

Table 3-1 Power supply unit parameters

Name	Description
Device Name	POE device name
PowerGoup ID	Power supply unit ID on device
PowerAdminStatus	Current power supply status of power supply unit
Power Max (W)	Maximum power allowed for power supply unit
Power Average (W)	Average power supply of power supply unit
Power Peak (W)	Maximum power provided
Power Free (W)	Currently available power supply

Table 3-2 Parameters of PoE port information

Name	Description
Device Name	POE device name
Power Group ID	Power supply unit ID of device
Port Descr	Description of device port
PortAdminStatus	Administration status for port: UP and DOWN
Port Priority	Power supply priority for port
Port Max (W)	Maximum power allowed for power supply unit
Power Average (W)	Average power supply of power supply unit
Power Peak (W)	Maximum power supply provided
Power Free (W)	Currently available power supply

3.7 Transceiver Browsing

In the function window, click "+" on the [Port Management] node and double-click the extended leaf node [Transceiver Browsing]. The system displays the [Transceiver Browsing] dialog box, as shown in Figure 3-8.

In the [Transceiver Browsing] dialog box, you can view detailed information about all transceivers on the device.

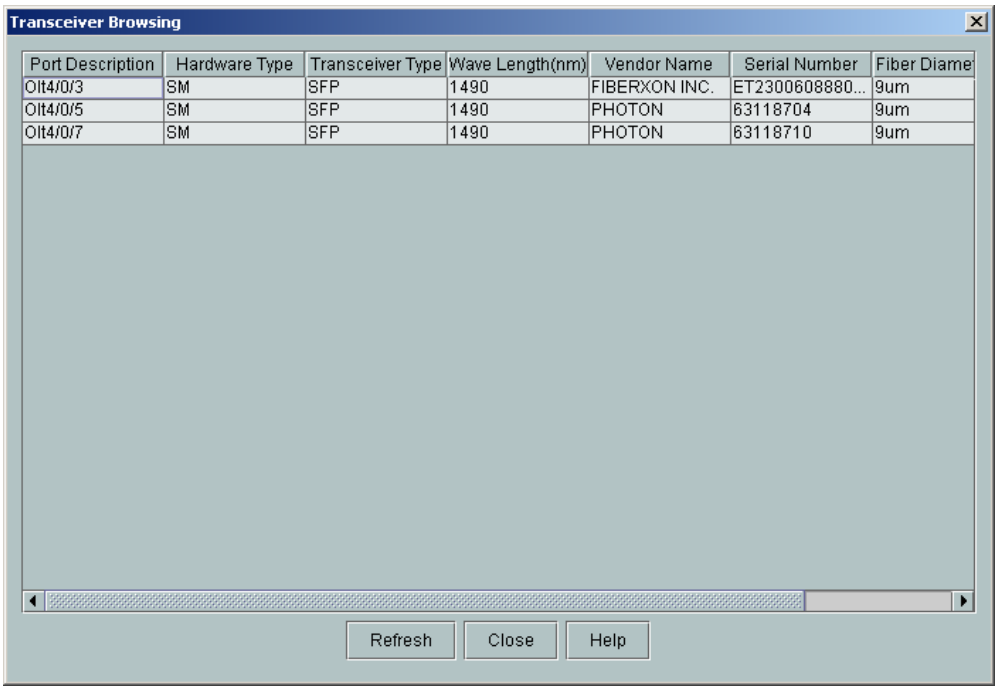


Figure 3-8 Transceiver Browsing

Table 3-3 lists parameters and their means in the [Transceiver Browsing] dialog box.

Table 3-3 Description of transceiver parameters

Parameter	Description
Port Description	Description of transceiver port
Hardware Type	Transceiver hardware type, including Single Mode (SM) and Multi-Mode (MM).
Transceiver Type	Transceiver interface type, including SFP, XFP, and GBIC.
Wave Length (nm)	Length of optical wave sent or received by the transceiver.
Vendor name	Name of transceiver vendor.
Serial Number	Product serial number of the transceiver.

Parameter	Description
Fiber Diameter Type	Diameter of the fiber connected with the transceiver. Options include 9um fiber, 50um fiber, 62.5um fiber, and copper wire.
Transfer Distance (m)	Maximum transmission distance of the signal sent by the transceiver.

3.8 Port Isolation

Port isolation is to add multiple ports into an isolation group to isolate the communication between ports, that is, ports in the same isolation group cannot send packets to or receive packets from each other.

In the function window, click "+" on the [Port Management] node and double-click the extended leaf node [Port Isolation]. The system displays the [Port Isolation] dialog box, as shown in Figure 3-9.

The [Port Isolation] dialog box displays the number of existing port isolation groups on the current device and their basic information. You can create a port isolation group, modify, refresh, or delete an existing port isolation group by clicking buttons at the bottom of the dialog box.

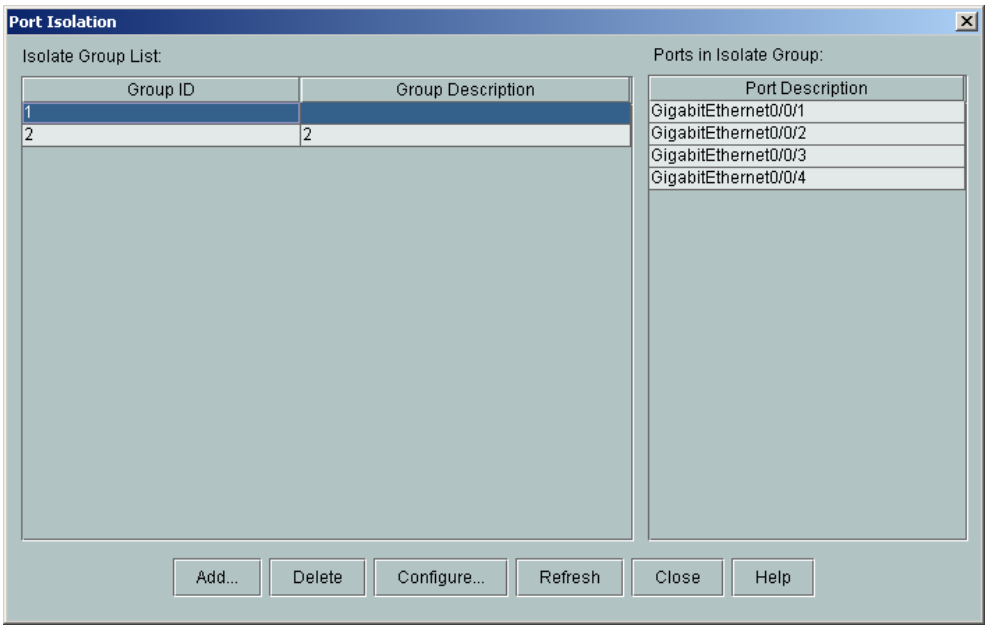


Figure 3-9 Port Isolation

In the [Port Isolation] dialog box, click <Add…> to open the [Add Port Isolate Group] dialog box. Enter an idle port isolation group ID and description. The group ID must fall into the permitted value range and the description can be null. Select a destination port, and then click <OK>. Alternatively, you can directly click <OK> without selecting a

destination port. If the group is added successfully, the isolation group information on the dialog box will be refreshed.

In the [Port Isolation] dialog box, select an isolation group. The right pane of the dialog box will display the general information about isolated ports in this isolation group. You can click <Configure…> and then modify the description and ports of this port isolation group in the popup [Configure Port Isolate Group] dialog box.

You can also select a port isolation group you do not need, and then click <Delete> to confirm and delete it.

Chapter 4 VLAN Configuration

4.1 Overview

Virtual Local Area Network (VLAN) is the protocol used to solve the problems of Ethernet broadcast and security. VLAN protocol adds a 4-byte 802.1Q frame header after the source address of an Ethernet frame, and uses VLAN ID to divide the users into small work groups, each group being a VLAN. The benefit of VLAN is to limit the broadcast range and form virtual work group, so as to manage the network dynamically.

Before the evolution of VLAN, people used to segment the network to improve the performance of the LAN or to limit the rights of inter-visiting among the computers on the network. At that time, each segment had its own network hardware which cannot be shared between segments. Nowadays, network can be segmented through VLAN and different segments can share a set of network hardware, thus, the spending on hardware is saved, meanwhile the workload in the moving of computers and the cost of network interconnection are reduced.

Quidview Device Manager supports the VLAN configuration management on the series Ethernet switches. The functions are mainly: VLAN management, VLAN virtual interface management, VLAN Trunk management and Isolate-VLAN management. This chapter discusses the VLAN configuration management of Quidview Device Manager.

4.2 VLAN Management

4.2.1 Adding a Layer 2 VLAN

Start the Quidview Device Manager, and select [Device /Open…] or click the button on the toolbar to open the panel view of a switch. Then select [VLAN Management/ Layer 2 VLAN Management] node from the function window to open the [Layer 2 VLAN Management] dialog box, as shown in Figure 4-1.

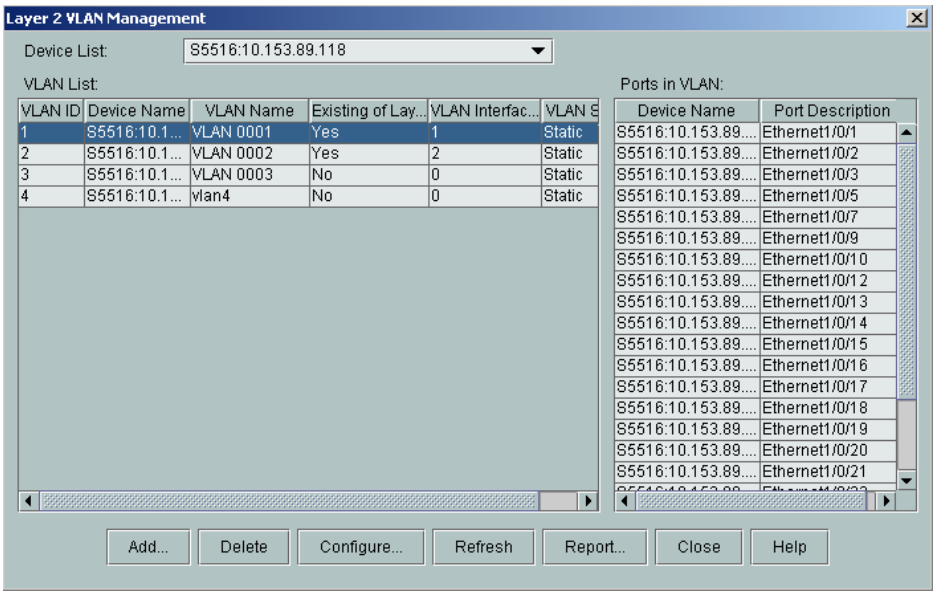


Figure 4-1 Layer 2 VLAN Management

The [Layer 2 VLAN Management] dialog box is the main interface to perform the VLAN configuration and management. The dialog box displays the number of VLANs existing on the switch and their basic information. Using the buttons at the bottom of the interface, the user can create, configure or delete a Layer 2 VLAN.

Click <Add…> in the dialog box, and the [Add VLAN] dialog box will appear, as shown in Figure 4-2. Input the related parameters in the boxes and click <OK>, and thus a new Layer 2 VLAN is created.

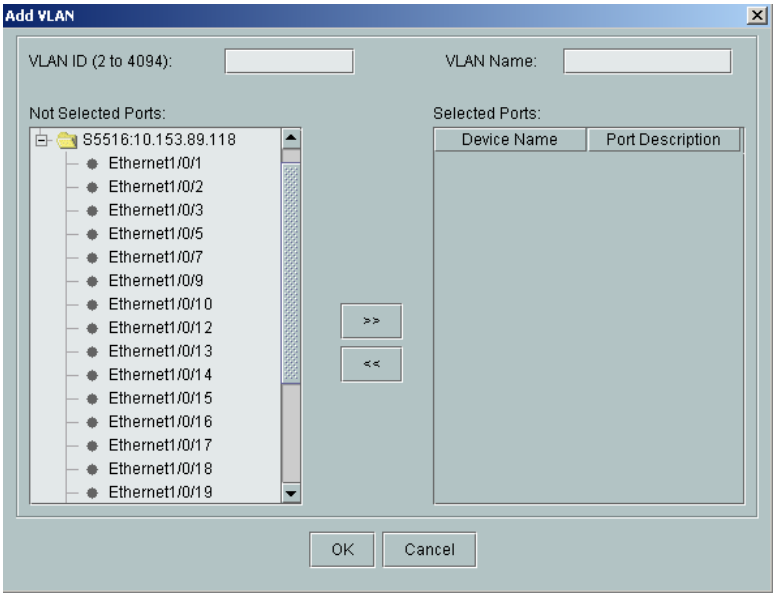


Figure 4-2 Adding a Layer 2 VLAN

The meaning of the parameters involved in the process is shown in Table 4-1.

Table 4-1 Description on the main parameters used for adding a Layer 2 VLAN

Parameter	Description
VLAN ID	Unique identifier of a VLAN, an integer from 2 to 4094.
VLAN name	Brief description of the functions or characteristic of VLAN, being a string less than 40 characters. It is optional during the process of creating a VLAN.
Selected ports	When creating a VLAN, you can specify the port list in the VLAN by selecting the ports to be contained in the VLAN from the [Not Selected Ports] list and click <>>>.

Note:

- The quantity of VLANs supported by the Ethernet switches varies with the device models, for example, S3026 supports 32 VLANs, S3026E supports 256 VLANs, while S3026F supports 4096 VLANs. For the number of VLANs supported by the device, see the corresponding user manuals.
- When creating a VLAN, the user may not specify a port. When configuring the VLAN attributes or adding the ports to the VLAN, the user can modify the ports contained in the VLAN. For details, please see the following sections.
- Trunk and Hybrid ports cannot be added to or deleted from VLAN.

4.2.2 Configuring a Layer 2 VLAN

Select a VLAN from the [Layer 2 VLAN Management] dialog box and click <Configure…>, and then the [Configure VLAN] dialog box will pop up. You can modify the VLAN name and the ports contained in the VLAN.

Note:

- When adding/deleting ports to/from the VLAN, the user can select a group of consecutive ports by pressing <Shift>, or select a group of inconsecutive ports by pressing <Ctrl>.
- VLAN 1 is the default VLAN and its attributes cannot be configured.

4.2.3 Layer 2 VLAN Report

In Figure 4-1, click <Report…> to open the saving file dialog box. Here enter the proper file name to save the VLAN information of current device to a text (*.txt) or HTML (*.html) file.

4.2.4 Deleting a Layer 2 VLAN

In the [Layer 2 VLAN Management] dialog box shown in Figure 4-1, select one or more VLANs to be deleted, and click <Delete> to delete them. After a VLAN is deleted, its ports will automatically return to the default VLAN, that is, VLAN 1.

⚠ **Caution:**

The default VLAN (VLAN 1) cannot be deleted.

4.3 VLAN Interface Management

4.3.1 Adding a VLAN Interface

To implement the network layer function on a VLAN interface, the user can specify a virtual interface to a VLAN, that is, to configure the IP address and mask for a VLAN.

Select [VLAN Management/VLAN Interface Management] in the function window to display the [VLAN Interface Management] dialog box, as shown in Figure 4-3.

VLAN Interface Management functions to manage VLAN interfaces. This dialog box displays the quantity of VLAN interfaces existing in the current device and their basic information. By clicking the buttons at the bottom of the interface, the user can create, configure or delete a VLAN interface.

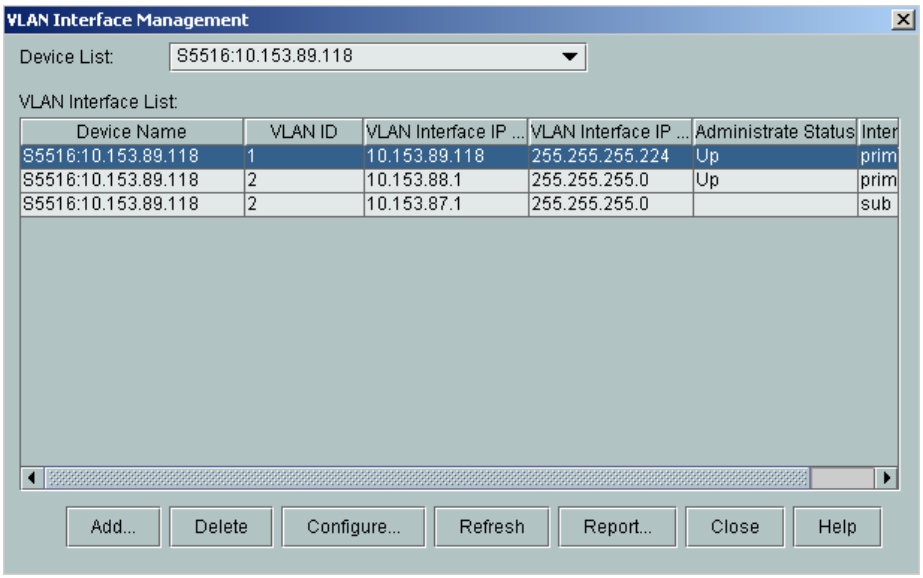


Figure 4-3 VLAN Interface Management

Click <Add…> on the interface to open the [Add VLAN Interface] dialog box, as shown in Figure 4-4. Input proper parameters, and click <OK>.

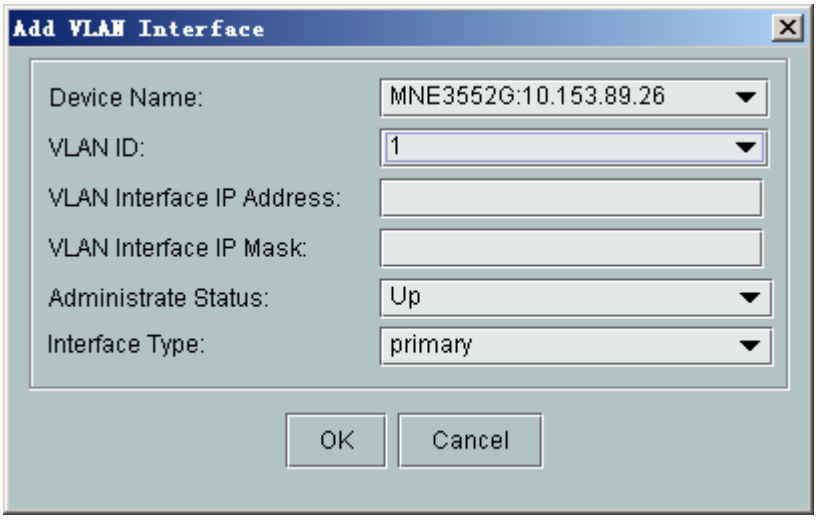


Figure 4-4 Adding a VLAN interface

4.3.2 Configuring a VLAN Interface

In the [VLAN Interface Management] dialog box shown in Figure 4-3, select a VLAN interface item and click <Configure…>, and then the [Add VLAN Interface] dialog box appears. The user can modify the IP address, mask or administrate status of the VLAN interface as needed.

4.3.3 VLAN Interface Report

In Figure 4-3, click <Report…> to open the saving file dialog box. Here enter the proper file name to save the VLAN interface information of current device to a text (*.txt) or HTML (*.html) file.

4.3.4 Deleting a VLAN Interface

To delete a VLAN interface, select a VLAN interface to be deleted from the [VLAN Interface Management] dialog box shown in Figure 4-3 and click <Delete>.

⚠ **Caution:**

Deleting a VLAN interface in use will break the connection between the system and the managed device.

4.4 VLAN Trunk Management

If a port is set as a Trunk port and some VLANs are allowed to pass through the port, the packets of the specified VLANs will pass through the port. Consequently, the multiple VLANs on this switch can interconnect with the corresponding VLANs on the remote switch.

4.4.1 Adding a VLAN Trunk

Click "+" on the [VLAN Management] node in the function window, and double-click the extended leaf node [VLAN Trunk Management]. Then, the [VLAN Trunk Management] dialog box will pop up, as shown in Figure 4-5.

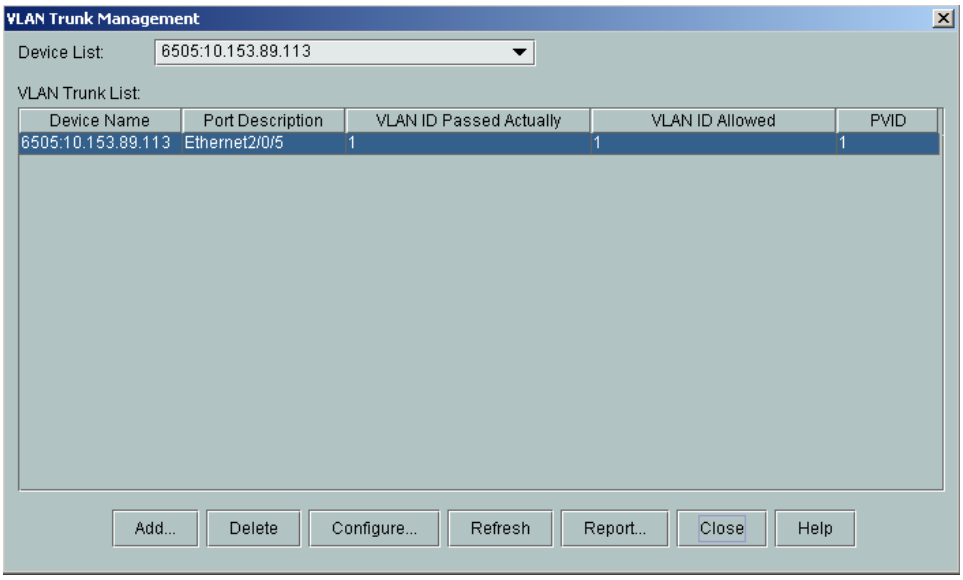


Figure 4-5 VLAN Trunk Management

The [VLAN Trunk Management] dialog box is the main interface to implement the VLAN Trunk management. The interface displays the quantity of VLAN Trunk ports existing in the current device and their basic information. By clicking the buttons at the bottom of the interface, the user can create a VLAN Trunk port, configure or delete an existing VLAN Trunk port.

Click <Add…> in the interface, and the [Add Trunk Port] dialog box will pop up, as shown in Figure 4-6.

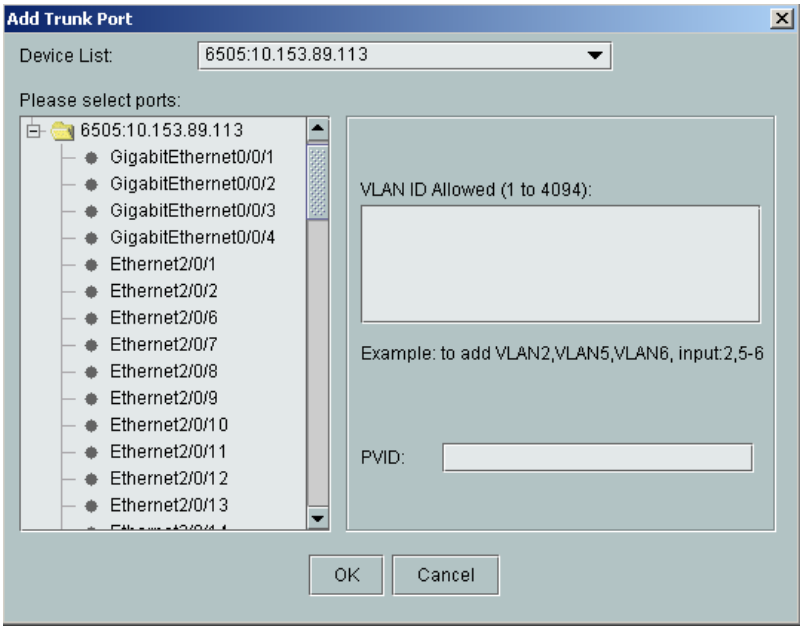


Figure 4-6 Add Trunk Port

The user needs to select a port or several ports form the port list on the left and specify the ID of the VLANs that can pass through the Trunk port in the edit box on the right, and then click <OK> to add a VLAN Trunk port.

Note:

- If the user chooses several ports and creates them as Trunk ports at one time, in the case that there is a Trunk port among the ports, the creation will not work.
- If there are Hybrid ports in current device, you should delete all of them before configuring a VLAN Trunk port.

4.4.2 Configuring a VLAN Trunk

The function of configuring VLAN Trunks is mainly to modify the list of the VLANs that can pass through the Trunk port. Select a data item in the interface shown in Figure 4-5, and click <Configure…>, and then the [Configure Trunk Port] dialog box will pop up. By editing the list of the passable VLANs in the text box, the user can perform the configuration of the existing Trunks.

4.4.3 VLAN Trunk Report

In Figure 4-5, click <Report…> to open the saving file dialog box. Here enter the proper file name to save the VLAN Trunk information of current device to a text (*.txt) or HTML (*.html) file.

4.4.4 Deleting a VLAN Trunk

Select a Trunk port to be deleted from the [VLAN Trunk Management] dialog box shown in Figure 4-5, and click <Delete> to delete the specified Trunk port.

4.5 VLAN Hybrid Management

This function is used to configure the tagged and untagged VLAN lists through a certain port.

4.5.1 Adding a VLAN Hybrid Port

In the function window, click on "+" corresponding to the [VLAN management] node, and double-click on the [VLAN Hybrid Management] leaf node to open the [VLAN Hybrid Management] dialog box, as shown in Figure 4-7.

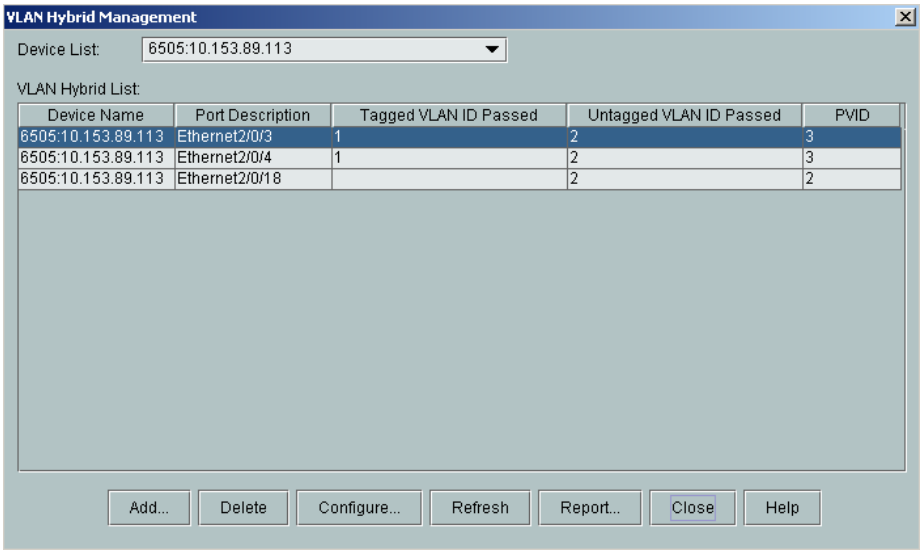


Figure 4-7 VLAN Hybrid Management

This dialog box implements VLAN hybrid management. It shows the number of VLAN hybrid ports on current device and the basic information of each port. With the buttons on the bottom of the interface, you can create a VLAN hybrid port, or configure/delete an existent one.

Click <Add…> to open the [Add Hybrid Port] dialog box, as shown in Figure 4-8:

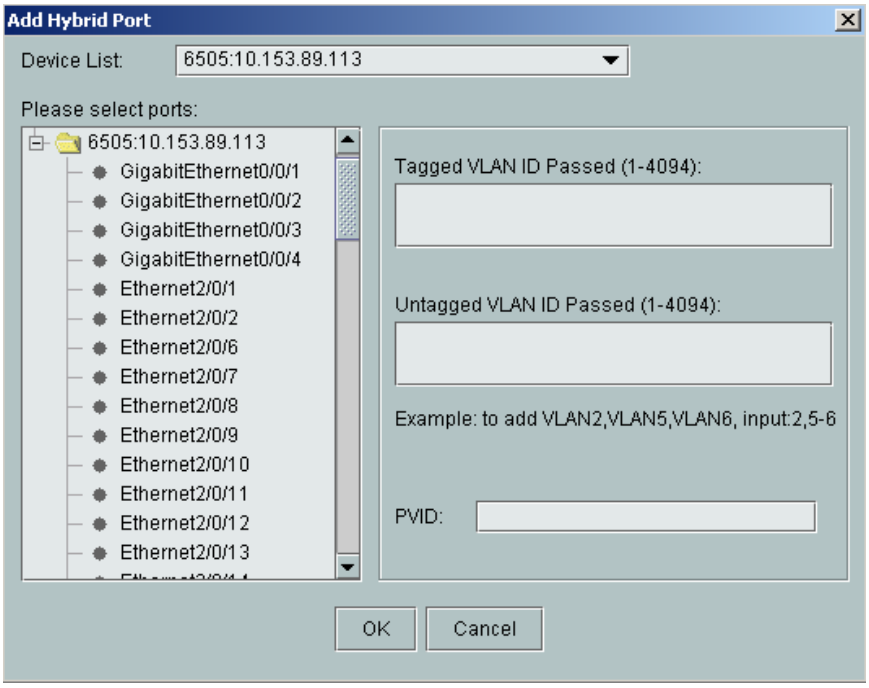


Figure 4-8 Adding a VLAN hybrid port

Select one or more ports from the left device port list, type the tagged VLAN ID, untagged VLAN ID and PVID through the port (s) in the right edit boxes, and click <OK> to create a new VLAN hybrid port.

Note:

If current device has Trunk ports, you must delete all of them before configuring a VLAN hybrid port.

4.5.2 Configuring a VLAN Hybrid Port

This function mainly modifies the tagged VLAN ID, untagged VLAN ID and PVID through the VLAN hybrid port. In Figure 4-7, select a data item and click <Configure…> to open the [Configure Hybrid Port] dialog box, where you can modify the tagged VLAN ID, untagged VLAN ID and PVID through the VLAN hybrid port. Click <OK> to finish the modification.

4.5.3 VLAN Hybrid Report

In Figure 4-7, click <Report…> to open the saving file dialog box, where enter a proper file name to save the VLAN hybrid information of current device to a text (*.txt) or HTML (*.html) file.

4.5.4 Deleting a VLAN Hybrid Port

In Figure 4-7, select a hybrid port and click <Delete>. After confirmation, the specified hybrid port will be deleted.

4.6 Isolate-VLAN Management

4.6.1 Introduction to Isolate-VLAN

Isolate-VLAN (Primary VLAN) adopts the structure of Layer 2 VLAN. An Isolate-VLAN corresponds to several SVLANs (Secondary VLANS) on an Ethernet switch. The Isolate-VLAN contains all the ports and uplink ports of the corresponding SVLANs, therefore the upper layer switch only needs to identify the Isolate-VLAN on the lower layer switch, instead of identifying the SVLANs contained in the Isolate-VLAN, thus simplifying the configuration and saving VLAN resource. To implement L2 packet separation among different users with Isolate-VLAN, you can allocate each user with an SVLAN containing the connection ports and uplink ports of the user. To achieve L2 packet interconnection among these users, you can simply group the connection ports of the users into an SVLAN.

4.6.2 Adding an Isolate-VLAN

In the function window, click on "+" corresponding to the [VLAN management] node, and double-click on the [Isolate-VLAN Management] leaf node to open the [Isolate-VLAN Management] dialog box.

Click <Add…> in the interface, and the [Add an Isolate-VLAN] dialog box will appear. The dialog box displays the VLANs existing in the current device. Select one of the VLANs and click <OK> to set the VLAN as an Isolate-VLAN.

4.6.3 Configuring an Isolate-VLAN

After creation, the user needs to configure the Isolate-VLAN and the SVLANs it contains.

In the [Isolate-VLAN Configuration] dialog box, select one by one the VLANs to be added into the Isolate-VLAN from the VLAN list, and click <Add…> to add the selected VLANs into the Secondary VLANs of the Isolate-VLAN. Click <Configure…> to write the data into the device, and thus the configuration of Isolate-VLAN is completed.

Note:

The Isolate-VLAN and SVLAN must contain physical ports which can't be VLAN Trunk, or the configuration for the Isolate-VLAN will fail.

4.6.4 Deleting an Isolate-VLAN

Select an Isolate-VLAN to be deleted from the dialog box and click <Delete> to delete a designated Isolate-VLAN, meanwhile, the deleted Isolate-VLAN and its Secondary VLANs will become the common VLANs of the current switch again.

4.7 Adding a Port to VLAN

With this function, the user can add a port or a group of ports to a specified VLAN. The operation method is as follows:

Select a port or choose a group of ports by pressing <Ctrl> from the device panel view, and select [VLAN Management/Add Ports to VLAN] or select [Add Ports to VLAN] from the right-click popup menu to open the [Add Ports to VLAN] dialog box, as shown in Figure 4-9.

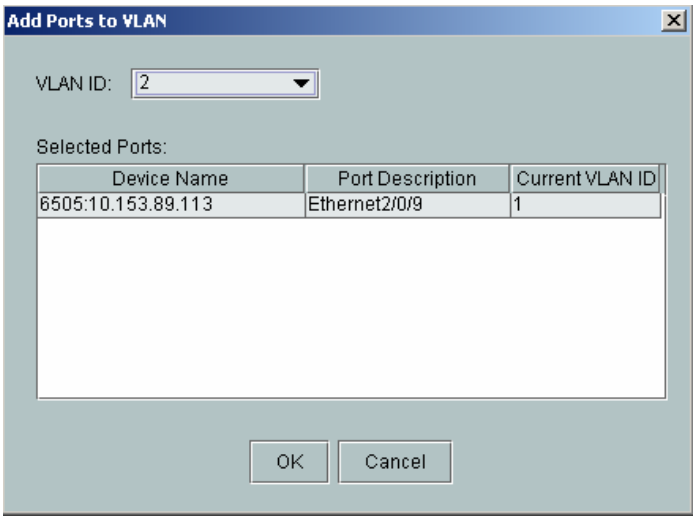


Figure 4-9 Adding a port to VLAN

Select the VLAN ID to which the port is to be added from the list, and click <OK> to add the port to the VLAN.

Caution:

VLAN1 is the default VLAN of the device and you cannot add a port to it.

4.8 Protocol VLAN Management

4.8.1 Adding a Protocol VLAN

In the function window, click “+” on the [VLAN Management] node and double-click the expanded [Protocol VLAN Management] leaf node, and then the [Protocol VLAN Management] dialog box appears, as shown in Figure 4-10.

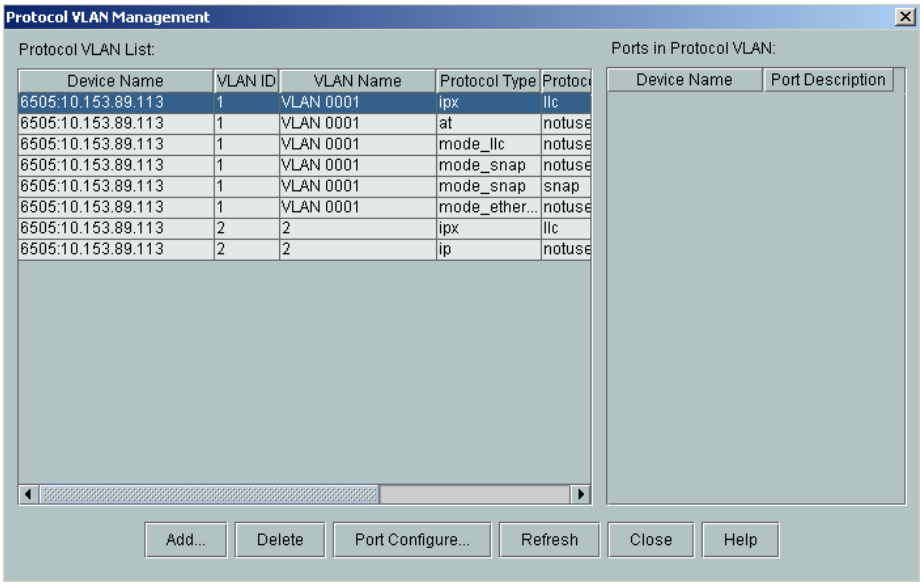


Figure 4-10 Protocol VLAN Management

The dialog box displays the existing protocol VLANs on the current device and their basic information. The buttons at the bottom of the interface enable you to create a protocol VLAN, and configure or delete an existing protocol VLAN.

Click <Refresh>, and the protocol VLAN information is refreshed.

Click <Add…>, and the [Add Protocol VLAN] dialog box appears, as shown in Figure 4-11.

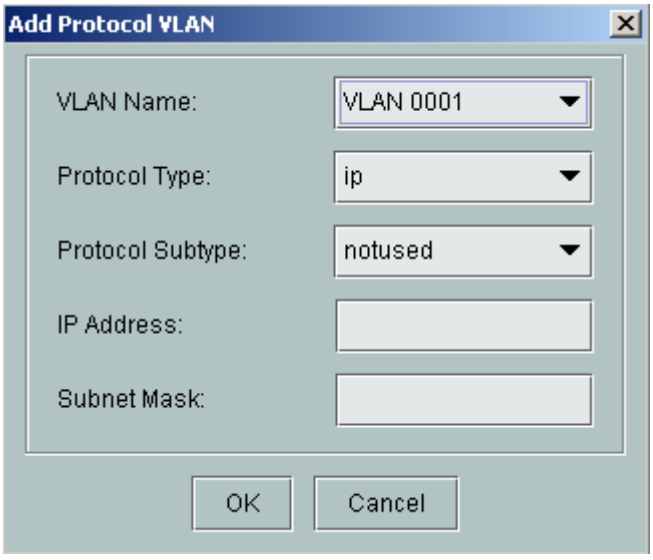


Figure 4-11 Add Protocol VLAN

Input related parameters and click <OK>, and you can create a protocol VLAN. The following parameters need to be configured.

- VLAN Name: Indicates for which VLAN to create a protocol VLAN.

- Protocol Type: Specifies a protocol type on which VLAN is based. Protocol types include ip, ipx, at, mode_llc, mode_snap and mode_etherneti.
- Protocol Subtype: Specifies on which sub-protocol among protocol types VLAN is based.

VLANs based on different protocol types need to be configured with different parameters:

- IP-based VLAN requires IP address and subnet mask.
- mode_llc-based VLAN requires dsap value which is the destination service access point in the range of 0 to FF and ssap value which is the source service access point in the range of 0 to FF.
- mode_snap- or mode_ethernetii- based VLAN requires protocol value in the range of 600 to FFFF if etype is selected for Protocol Subtype.
- VLANs based on other protocols do not require any other parameters.

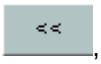
Note:

For different types of devices, there is a limit to the number of protocol VLANs to be created for one VLAN and to the total number of protocol VLANs for a device.

4.8.2 Configuring a Protocol VLAN

The main feature of protocol VLAN configuration is to modify protocol VLAN ports.

In the [Protocol VLAN Management] dialog box, select one row of data item and click <Port Configure…> to open the [Protocol VLAN Config] dialog box, as shown in Figure 4-12. By clicking

or 

, you can add/delete one port or a group of ports to/from the VLAN. Click <OK> to complete modifying the protocol VLAN ports.

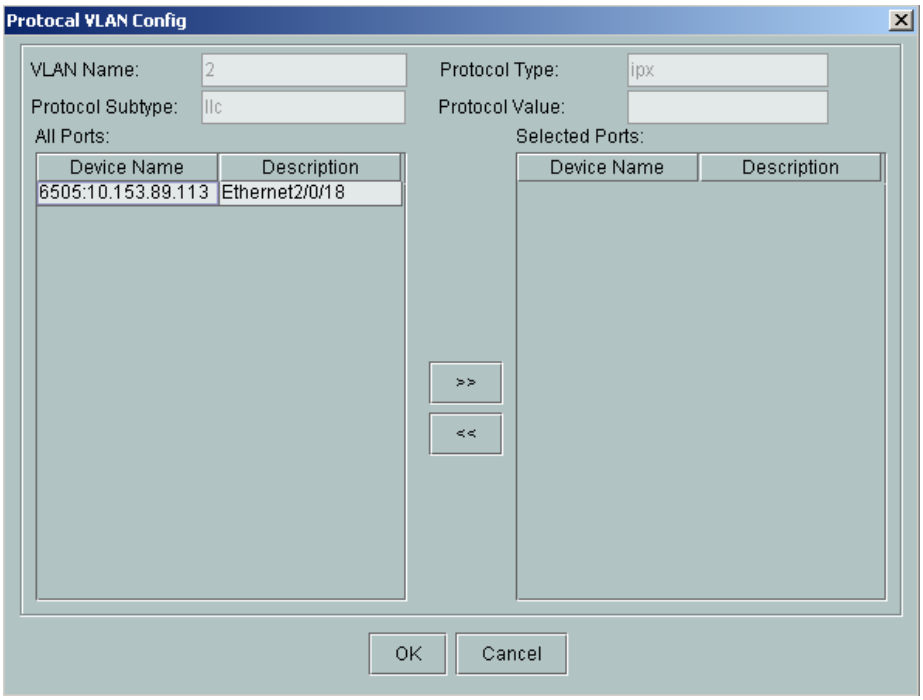


Figure 4-12 Protocol VLAN Config

Note:

- If a protocol VLAN is already dispatched to a port, this protocol VLAN cannot be deleted. Cancel the configuration before deletion.
- Protocol VLAN configuration is only available for a hybrid port, and cannot be deleted on a configured non-hybrid port.

4.9 Voice VLAN Management

Voice VLAN is a special VLAN for voice streams of users. You can decide whether a data stream is an IP phone data stream based on the source MAC address of the stream passing through the port. You can configure the organizationally unique identifier (OUI) address in advance or use the default one as the criteria. OUI address indicates the address of a certain manufacturer.

Voice VLAN configurations include:

- Enabling/Disabling voice VLAN feature
- Configuring the voice VLAN attributes of the port
- Configuring the OUI address identified by the voice VLAN
- Configuring the security mode of the voice VLAN
- Configuring the auto mode of the voice VLAN

- Configuring the aging time of the voice VLAN

In the function window, click “+” on the [VLAN Management] node and double-click the expanded [Voice VLAN Management] leaf node, and then the [Voice VLAN Management] dialog box appears, as shown in Figure 4-13.

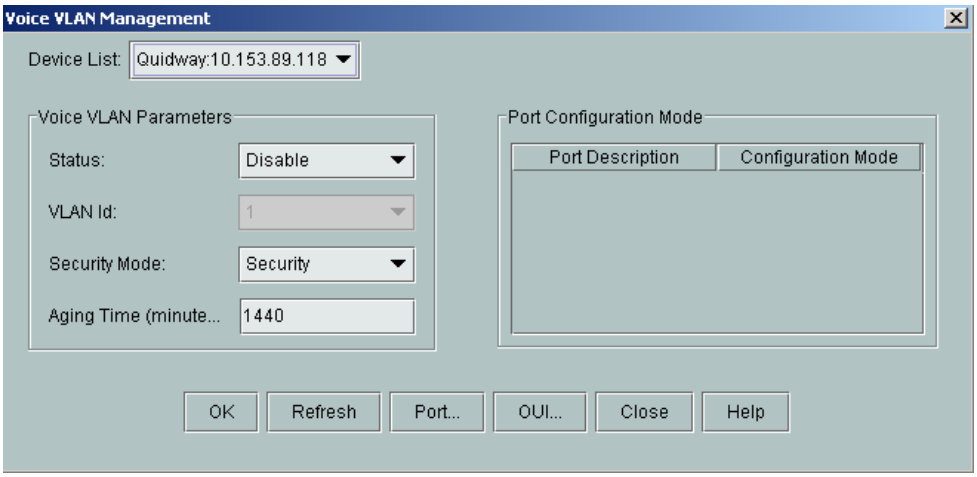


Figure 4-13 Voice VLAN Management

This dialog box is the main interface to implement voice VLAN management. It displays the parameters and basic information of the existing voice VLANs on the current device.

Configuring Voice VLAN

In the [Voice VLAN Management] dialog box, configure proper parameters and click <OK>.

🕮 **Note:**

- The default VLAN cannot be configured as a voice VLAN.
- Only one VLAN is allowed to be configured as a voice VLAN.
- If the security mode is set to **Security**, only the streams with the specified OUI addresses are allowed to pass the port.

4.9.1 Configuring Voice VLAN Ports

The port configuration mode table lists the ports on which voice VLAN is enabled.

In auto configuration mode, when IP phone streams pass an enabled voice VLAN port, the switch can identify the untagged OUI packets based on the automatically learned source addresses, add the port to the voice VLAN automatically and add an ACL to the port. In manual mode, because the switch cannot identify OUI packets and add the port

to the voice VLAN automatically, you must add the desired port to the voice VLAN manually.

The operation steps for adding a port to an enabled voice VLAN are as follows:

In the [Voice VLAN Management] dialog box, click <Port…> to open the [Voice VLAN Port Configuration] dialog box. Select one or more ports, and then click to add them to the [Enabled Ports] area. Click <OK> to complete the configuration. In the [Port Configuration Mode] area, you can set the configuration mode to Auto or Manual.

4.9.2 OUI Configuration

Voice VLAN identifies the IP phone terminal devices from different manufacturers through source MAC addresses. OUI is the first three bytes of an MAC address and is assigned to each organization by Institute of Electrical and Electronics Engineers (IEEE).

In the [Voice VLAN Management] dialog box, click <OUI…> to open [OUI Configuration] dialog box. Click <Create> to open the [New OUI Address] dialog box. Input an OUI address, a mask and a description. The first three bytes of the address are defaulted as the valid length of the OUI, and the left parts serve as the mask of the MAC address.

The system supports up to 16 OUI addresses.

Chapter 5 Protocol Management

5.1 Overview

Quidview Device Manager supports the configuration of multiple Layer 2 protocols, such as STP, GARP, GVRP, GMRP, IGMP Snooping and MSTP. This section briefly introduces the above Layer 2 protocols first, and then proceeds to elaborate the configuration of these protocols. If you are not familiar with these protocols, you may consult the related documentation.

5.1.1 STP/RSTP

Spanning Tree Protocol (STP) is a part of bridging protocol of IEEE 802.1D. The basic idea is to span a “tree”, and the root is called root bridge. Different switches can be selected as the root tree according to different settings, while there is only one root bridge at one time. Starting from the root bridge, a tree is spanned level by level. The root bridge sends configuration packets periodically, and non-root bridge receives and forwards configuration packets. If a switch can receive configuration packets from more than one port, it means that there are at least two paths from the port to the switch, thus forming a circular loop. Then the switch will select a port according to the configuration of the port and block other ports to remove the circular loop. If a port has not received the configuration packets for a long time, the switch will regard that the configuration of the port expires and the network topology might have changed, and it will recalculate the network topology and span a new tree. STP mainly has the following functions:

- Removing the network circular loop connection caused by mistake or by accident, thus avoiding the network broadcast storm resulted from network circular connection.
- Making it possible for the network to backup connections.

Ethernet switches apply the Rapid Spanning Tree Protocol (RSTP) which is an enhanced version of the STP. With the RSTP, the delay is shortened to a great extend under certain conditions when the root port and specified port enter the forwarding status, thus the time to stabilize the network topology is much shorter than before.

5.1.2 GARP

The Generic Attribute Registration Protocol (GARP) provides the means of distributing, propagating and registering some information (e.g., VLAN, multicast address) for the switch members in the same switching network.

The GARP itself is not an entity operating in the switch. The application entity conforming to the GARP is called a GARP application. At present the main GARP

applications are the GVRP (GARP VLAN Registration Protocol) and GMRP (GARP Multicast Registration Protocol). If a GARP application entity lies on a port of a switch, each port corresponds to a GARP application entity.

Via the GARP mechanism, the configuration information of a GARP will be propagated throughout the entire switching network. The GARP member can be either a terminal workstation or a bridge. The GARP member notifies other GARP members to register or unregister its attribute information by means of declaring or claiming declaration, and registers or unregisters the attribute information of other GARP members according to their declaration or claimed declaration.

The GARP members use message to carry out the information exchange. There are 3 types of GARP messages which are Join, Leave, and LeaveAll. When a GARP application entity wants to have some attribute information registered, it will send JoinIn message externally. If a GARP application entity hopes other GARP application entities to unregister some attribute information, it will send Leave message externally. After a GARP application entity starts, a LeaveAll timer will start. If timeout occurs, LeaveAll message will be sent externally, which enables other GARP application entity to re-register all the messages in this entity. By message interaction, all the attribute messages to be registered are propagated throughout all the switches in the same switching network.

The protocol data packets of the GARP application entity have special MAC addresses. After having received the packets from the GARP application entities, the switches supporting GARP features will differentiate the packets in terms of MAC addresses and deliver them to the corresponding application entities (GVRP or GMRP) for processing.

5.1.3 GVRP

The GARP VLAN Registration Protocol (GVRP) is an application of the GARP. Based on GARP operating mechanism, the GVRP maintains the dynamic VLAN registration information of the switches and propagates the information to other switches. All of the switches supporting GVRP features can receive the VLAN registration information from other switches and dynamically refreshes the local VLAN registration information, including the current VLAN members, and via which ports the VLAN members can arrive. All the switches supporting GVRP features can propagate the local VLAN registration information to other switches, so as to keep the consistency of the VLAN information of the devices supporting GVRP features in the same switching network. The VLAN registration information propagated by the GVRP contains both the local static registration information configuration manually and the dynamic registration information from other switches.

5.1.4 GMRP

The GARP Multicast Registration Protocol (GMRP) is an application of the GARP. Based on GARP operating mechanism, the GMRP maintains the dynamic multicast

registration information of the switches. All of the switches supporting GMRP features can receive the multicast registration information from other switches and dynamically refreshes the local multicast registration information, propagating the local multicast register information to other switches at the same time, so as to keep the consistency of the multicast information of the devices supporting GMRP features in the same switching network. The multicast registration information propagated by the GMRP contains both the local static multicast registration information configuration manually and the dynamic multicast registration information from other switches.

5.1.5 IGMP Snooping

Like the IGMP, the IGMP Snooping is also applied in the management and control of multicast group. They use the same packet, i.e., IGMP packet. The IGMP runs on network layer, while IGMP Snooping runs on link layer. When Layer 2 device receives the IGMP packet transmitted between the host and router, it will copy IGMP packets specially and transmits the copy to CPU, then the IGMP Snooping will analyze the information brought by the IGMP packets, then creates and maintains the MAC multicast address table on Layer 2. After this, the multicast packets issued by routers will be forwarded in terms of MAC multicast address. Only when IGMP Snooping has received the IGMP leave packet of a port, or when the timeout of the aging timer of a port occurs, can the IGMP Snooping send IGMP packets to the port, and all of the packets are special group query packets of IGMP. Otherwise, it does not send any packets to ports. Without the IGMP Snooping, multicast packets will be broadcast on Layer 2, and when implementing the IGMP Snooping, multicast packets will be multicast on Layer 2.

5.1.6 MSTP

MSTP (Multiple Spanning Tree Protocol) integrates STP and RSTP. MSTP associates VLAN and spanning tree and divides one switching network into multiple regions. Multiple spanning trees are formed in each region, and each spanning tree is independent. MSTP tailors the loop network into a non-loop tree network, in which way the packet hyperplasia and indefinite loop in the loop network can be avoided. It also provides multiple redundant paths for data forwarding so as to implement load sharing in the process of data forwarding. MSTP includes the following basic concepts:

MST Regions: Multiple Spanning Tree Regions are composed of the switches with the same region name, the same VLAN-spanning tree mapping configuration, and the same MSTP revision level in the switching network. There may be multiple MST regions in one switching network. The user can assigns multiple switches in one MST region by MSTP configuration command. For details, refer to Configuration Process in this Chapter.

IST: Internal Spanning Tree, one of the spanning trees inside MSTP region, constitutes CIST (Common and Internal Spanning Tree) of the whole switching network together with CST (Common Spanning Tree). IST is one fragment of CIST in MST region.

CST: Common Spanning Tree connects all single spanning trees in MST region of the switching network. If each MST region is regarded as one “switch”, CST is the spanning tree calculated by these “switches” via STP and RSTP.

CIST: Common and Internal Spanning Tree, composed of IST and CST, is the single spanning tree connecting all switches in the switching network.

MSTI (Multiple Spanning Tree Instance): multiple spanning trees can be generated in one MST region by the calculation of MSTP, and each spanning tree is independent. Each spanning tree is called one MSTI.

Region Root: The root of IST and MSTI in the MST region is called the region root. The topology of each spanning tree in MST region can be different, so is the root.

Common Root Bridge: The root switch of CIST is the Common Root Bridge.

Port Role: in the calculation process of MSTP, the port role can be specifying the port and the root port. The root port is the port to the root path with minimum cost. The specified port is the port responsible for forwarding data to LAN or other switches. The same port may act varying roles in different spanning tree instances.

Ethernet switches support MSTP and are compatible with switches supporting STP and RSTP. Both the protocol packets can be identified and applied in the calculation of the spanning tree by the switch applying MSTP.

5.2 Configuring the RSTP

5.2.1 Configuring the RSTP of a Device

I. Operation procedure

Click "+" on the [Protocol Management] node in the function window and double-click the extended leaf node [Device RSTP Protocol Configuration], and the [Device RSTP Protocol Configuration] dialog box will pop up, as shown in Figure 5-1.

Select a line or several lines of data to be configured, click <Configure…>, and input the proper data in the popup dialog box, and then click <OK> to complete the RSTP configuration of the device

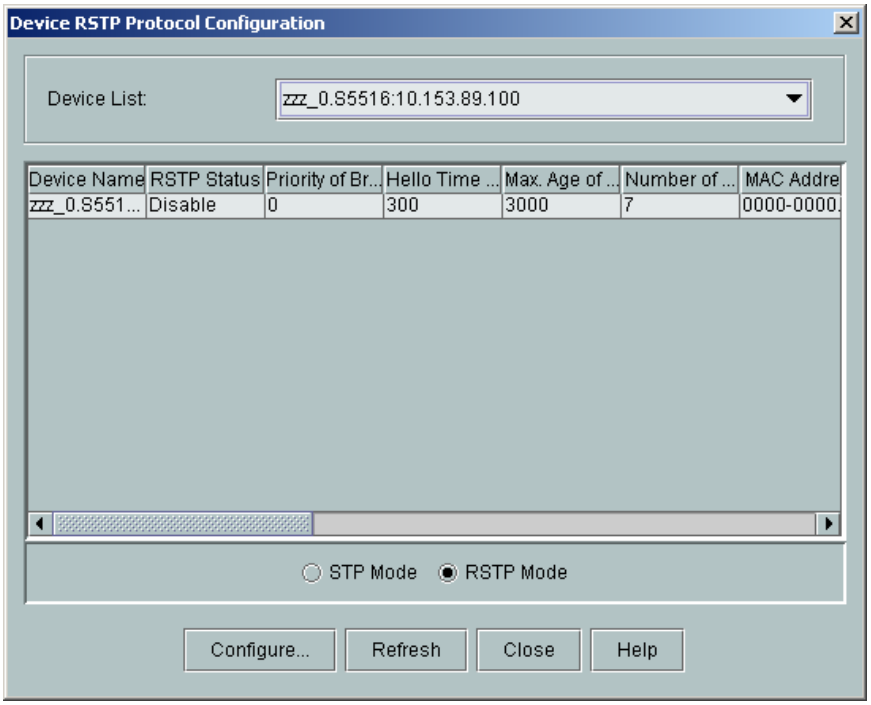


Figure 5-1 Device RSTP Protocol Configuration

II. Parameter description

1) RSTP Status

There are only two configurable options: Enable and Disable. To enable RSTP of the device, select “Enable”. To disable RSTP protocol of the device, select “Disable”.

Since partial network resource will be occupied after the STP feature of the device is enabled, RSTP is disabled by default.

2) Priority of Bridge

The priority of a bridge decides whether or not the bridge can be selected as the root of the entire spanning tree. The user can set a smaller value to specify a bridge as the root. If all the bridges in the entire switching network have the same value, the bridge with the smallest MAC address will be selected as the root. When the RSTP is enabled, if the priority of the bridges is configured, the spanning tree will be recalculated.

By default, the priority of bridge is 32768.

3) Hello Time of Bridge

The Hello Time is the interval of transmitting configuration messages among switches. A proper Hello Time value ensures that the bridge can find the link fault in the network in time, and it does not occupy much network resource. If Hello Time is too long, the bridge might regard that the link might have failed because of link discarded packets, and recalculates spanning tree. If Hello Time is too short, the bridge will send configuration messages frequently, adding load to network and CPU. It is recommended that the user should configure with the default value.

By default, Hello Time is 2 seconds.

4) Max Age of Bridge

Max Age is used to determine whether or not the configuration message is “dated”. If the parameter is too small, the calculation of spanning tree will become too frequent, and perhaps the network block will be taken as link fault. If the parameter is too large, the link fault might not be found in time, thus decreasing the auto-adaptive capability of the network. The user can configure according to the actual requirements. It is recommended that the user should configure with the default value.

By default, Max Age is 20 seconds.

5) Number of Bridges Between Two Nodes

Switching network has tree architecture without loop. Any two PC hosts are connected by a path passing a series of bridges. Network diameter is the path which has the greatest number of bridges and it is represented by the number of the bridges on the path. It is recommended that the number of the bridges between the two ends of the switching network should not exceed 7.

By default, the parameter is configured to 7.

6) MAC Address of Root bridge

MAC address of root switch in switch fabric

7) Startup protocol

Select startup STP protocol or RSTP protocol.

5.2.2 Configuring Port RSTP

By default, the RSTP is enabled on all ports after the device RSTP is started. To control the RSTP's operation flexibly, the user may disable the Spanning Tree features of specified Ethernet ports, so that these ports cannot participate in the calculation of spanning tree.

I. Operation procedure

Click "+" on the [Protocol Management] node in the function window and double-click the extended leaf node [Port RSTP Protocol Configuration], and the [RSTP Protocol Configuration] dialog box will pop up, as shown in Figure 5-2.

In this figure, select one or more lines of data to be configured and click <Configure…>. Enter the related data in the popup dialog box and click <OK> to complete the configuration of port RSTP. Click <Traffic Monitor>, access the dialog box of port traffic monitor and browse number of RSTP packets received and sent by the port. RSTP pockets are increasing constantly. When it comes to a certain number, it is not conveniently for you to browse. You can click <Clear Monitor Information> to clear previous RSTP pocket data.

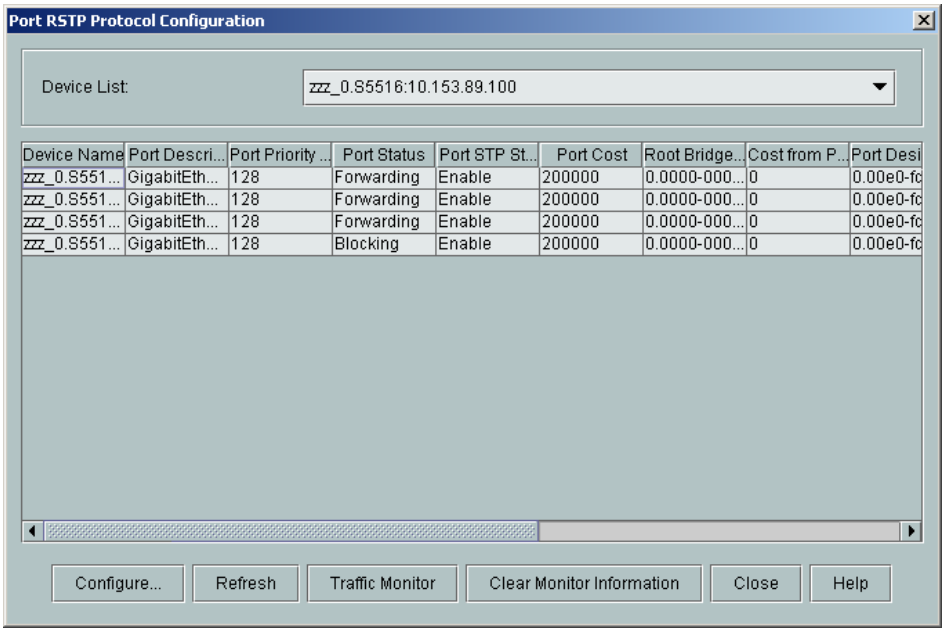


Figure 5-2 Port RSTP Protocol Configuration

II. Parameter description

1) Port Priority

By setting the priority of the Ethernet port, the user can designate a specified Ethernet port to be contained in a spanning tree. Generally, the smaller the value configured is, the higher the priority level is, the more likely it is that the Ethernet port is contained in the spanning tree. If all the Ethernet ports of the bridge have the same priority, the priority will be determined by the index of the port. Note that the change of the port priority will result in the recalculation of the spanning tree.

By default, the priority of all Ethernet ports is 128.

2) Port STP Status

The configuration item has two options: Enable and Disable. “Enable” means the port is available. “Disable” means the port is not available.

3) Port Cost

Cost value of a port is the path cost of the port, which is related to link speed. The faster the link speed is, the smaller the parameter should be configured. If the parameter is set to the default value, RSTP will automatically detect the link speed of the current Ethernet interface and converts it into the corresponding path cost. It is recommended that the user should use the default and let the RSTP itself calculate the path cost. Note that the configuration of the cost value of STP port will result in the recalculation of the spanning tree.

By default, the cost values of all Ethernet port of the bridge are set to 20000 when the port speed is 10 Mbps, and are set to 200 when the port speed is 100 Mbps.

5.3 Configuring the GARP

5.3.1 Configuring Global GARP

I. Operation procedure

Click "+" on the [Protocol Management] node in the function window and double-click the extended leaf node [Device GARP Protocol Configuration], and the [Device GARP Protocol Configuration] dialog box will pop up, as shown in Figure 5-3.

In Figure 5-3, select one or more lines and click <Configure…> to open a dialog box. Here select the status for the GVRP and GMRP, set the LeaveAllTime value, and click <OK> to finish global GARP configuration.

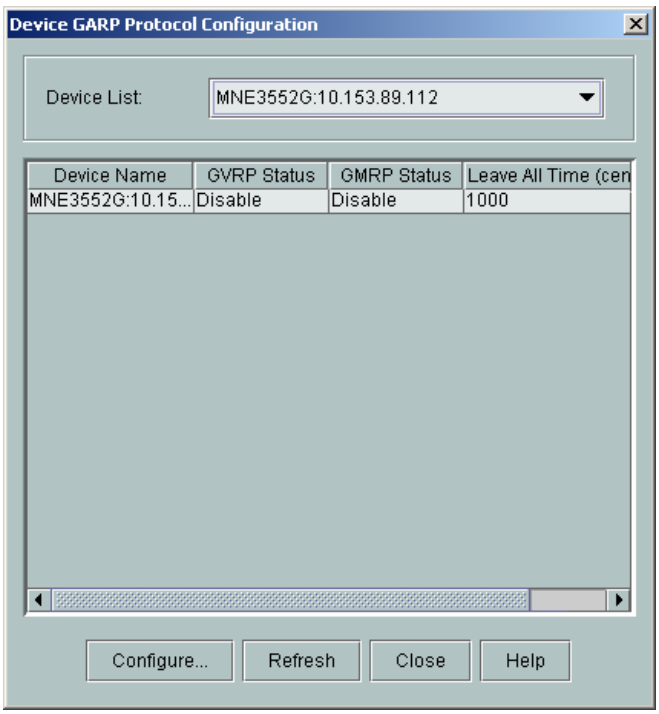


Figure 5-3 Device GARP Protocol Configuration

II. Parameter description

This dialog box is used to configure the global status of the GVRP and GMRP, that is, whether the global GVRP and GMRP is configured. The value of the Leave All Time (a timer) for the GARP ranges from 65 centiseconds to 32765 centiseconds and must be an integral multiple of 5. By default, it is 1000 centiseconds, namely 10 seconds. After Leave All Time timer timeout, each GARP application entity sends Leave All Time Message periodically, deleting the whole VLAN information on it.

By default, global GVRP and GMRP are disabled.

5.3.2 Configuring Port GARP

I. Configuring port GARP

Click "+" on the [Protocol Management] node in the function window and double-click the extended leaf node [Port GARP Configuration], and the [Port GARP Configuration] dialog box will pop up, as shown in Figure 5-4. In this dialog box, you can set the timer parameters of GARP, including Join Time, Leave Time, and Leave All Time.

1) In the figure, select one or more lines of data to be configured and click <Configure…>. In the popup dialog box, enter the related data and click <OK> to complete the configuration of port GARP.
2) Click <Traffic Monitor> to open the port traffic monitoring dialog box as shown in Figure 5-12, where you can browse the numbers of GARP packets received and sent on the port. As the number of GARP packets keeps increasing, you can click <Clear Monitor Information> to clear the history GARP packet data.

Note:

- The value of GARP timers will be used in all the GARP applications running in the same switching network, including GVRP and GMRP.
- The GARP timers on all the switches in the same switching network must have the same value; otherwise GARP application will not operate normally.
- In practice, you need to configure Leave Time more than two times of Join Time and less than Leave All Time; otherwise, an error will be prompted.

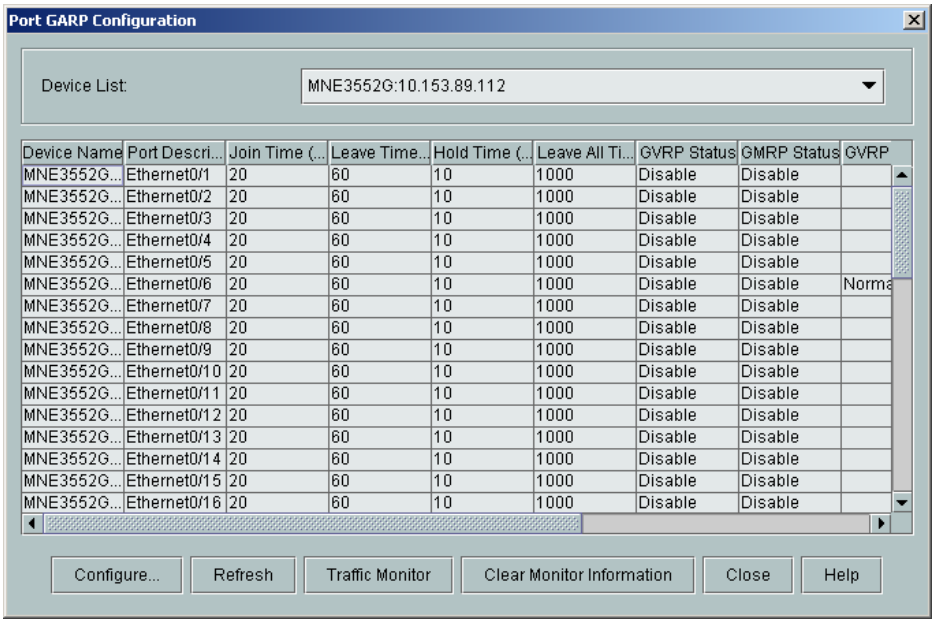

Port GARP Configuration
Device List:
MNE3552G:10.153.89.112
Device Name | Port Descri... | Join Time (... | Leave Time... | Hold Time (... | Leave All Ti... | GVRP Status | GMRP Status | GVRP
MNE3552G... | Ethernet0/1 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/2 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/3 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/4 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/5 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/6 | 20 | 60 | 10 | 1000 | Disable | Disable | Norma
MNE3552G... | Ethernet0/7 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/8 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/9 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/10 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/11 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/12 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/13 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/14 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/15 | 20 | 60 | 10 | 1000 | Disable | Disable
MNE3552G... | Ethernet0/16 | 20 | 60 | 10 | 1000 | Disable | Disable
Configure...
Refresh
Traffic Monitor
Clear Monitor Information
Close
Help

Figure 5-4 Port GARP Configuration

5.4 Configuring the IGMP Snooping

I. Operation procedure

Click "+" on the [Protocol Management] node in the function window and double-click the extended leaf node [IGMP Snooping Configuration] to open the [IGMP Snooping Configuration] dialog box, as shown in Figure 5-5.

Input the proper data in the protocol data edit box and click <Configure…> to complete the IGMP Snooping configuration of the device.

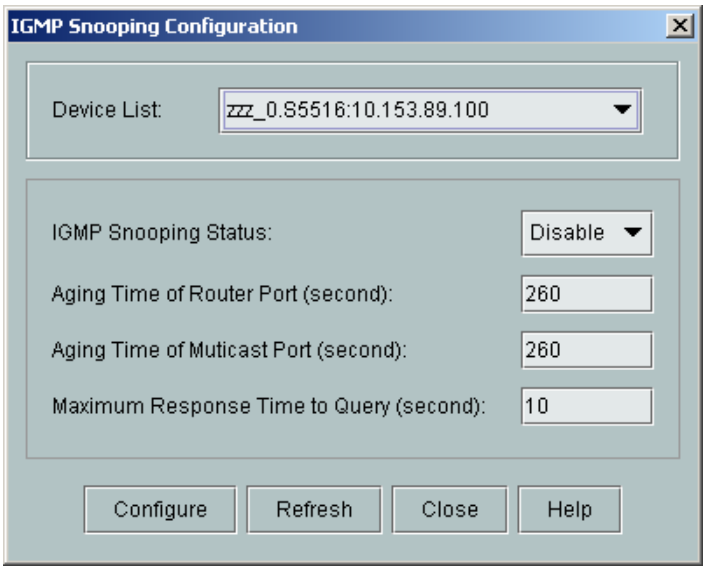


Figure 5-5 IGMP Snooping Configuration

II. Parameter description

1) IGMP Snooping Status

The IGMP Snooping status has two options: Enable and Disable, which are used to enable and disable the IGMP Snooping protocol of the device respectively.

By default, the IGMP Snooping is enabled.

⚠ **Caution:**

Because the IGMP Snooping and GMRP cannot operate at the same time, the user cannot enable the IGMP Snooping when the GMRP operates.

---

2) Aging Time of Router Port

The purpose of configuring aging time of router port is to delete a router port from the port members of all MAC multicast groups, if the port has not received general query packet of the router within the aging time of the router port.

By default, the aging time of router port is 260 seconds.

3) Maximum Response Time to Query

The purpose of configuring maximum time of response to query is to delete a port from the port members of a multicast group if the port has not received any report packet with the maximum time of response to query.

By default, the maximum time of response to query is 10 seconds.

4) Aging Time of Multicast Port

The purpose of configuring aging time of multicast port is to send specified group query to a port if the port has not received the report packets of a multicast group within the aging time of a host port.

By default, the aging time of multicast port is 260 seconds.

5.5 MSTP Protocol Configuration

5.5.1 MSTP Protocol Configuration

I. MSTP information list

Click "+" on the [Protocol Management] node in the function window and double-click the extended leaf node [MSTP Protocol Configuration] to open the [MSTP Configuration] dialog box, as shown in Figure 5-6. MSTP protocol configuration list includes the global MSTP information, MSTI information, and port MSTP information, which are detailed below respectively.

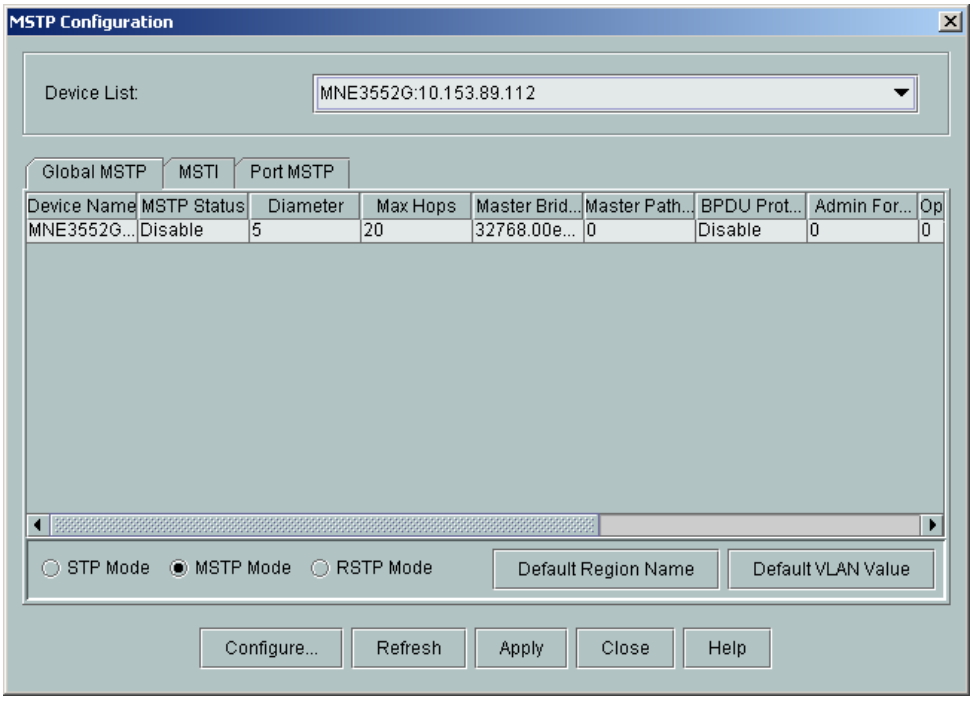


Figure 5-6 Global MSTP information

II. Default setting

There are two default configuration buttons in above figure: <Default Region Name> and <Default VLAN Value>.The former sets the first MAC address of the MST region switch and the latter makes all VLAN mapping MST instances to 0.

Caution:

To avoid the network oscillation, the protocol will not be validated as soon as it is configured. It must be enabled with <Apply> after all configurations are completed.

III. Global MSTP configuration

In Figure 5-6, select one line or multiple lines of data for configuration, and click <Configure…> to open the dialog box shown in Figure 5-7. Input the appropriate data in the dialog box, and click <OK> to complete the MSTP configuration for the device. In Figure 5-6, you can also click <Apply> to send a command to the device for activating the new MSTP configuration.

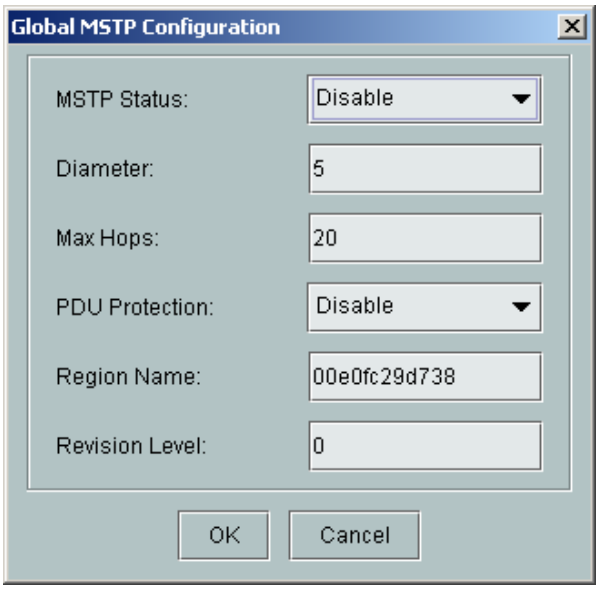


Figure 5-7 Global MSTP Configuration

IV. Parameters description

1) MSTP Status

There are only two options for the configuration entry: Enable and Disable, where “Enable” enables MSTP while “Disable” disables MSTP.

2) Diameter

The network diameter of the switching network is configured. Network diameter is the parameter representing the network scale. The more the network diameter is, the larger the network scale is. The configuration range of the network diameter is between 2 and 7.

3) Max Hops

It is also called the maximum hop counts of the MST region, which limits the scale of MST region. The maximum hop counts configured on the region root also acts as the maximum hop counts of MST region. As long as the forwarded configuration message (BPDU) in the region passes each switch from the root switch of the spanning tree, the hop counts will deduct 1. The switch discards the received configuration message with the hop count of 0, and the switch outside the maximum hop counts cannot forward the data because it cannot participate in the calculation of the spanning tree, consequently limiting the scale of MST region. The larger the maximum hop count of MST region is, the larger the scale of MST region is.

The scale of MST region can be limited only when the maximum hop count of switch MST region is configured. Other switches in MST region will adopt the configuration on the region root, although the switch is configured accordingly. The maximum hop counts of the MST region are between 1 and 40.

4) BPDU Protection

For access layer device, the access port is usually connected to the user terminal (such as PC) or the file server, when the access port is set as the edge port to implement the fast migration of these ports. When these ports receive the configuration message (BPDU packet), the system will automatically set these ports as non-edge ports and re-calculate the spanning tree so as to cause the oscillation of the network topology. Normally, these ports will not receive the configuration message of the spanning tree protocol. If someone forges the configuration message to attack the switch viciously, the network oscillation will occur. BPDU monitoring function may prevent such network attack. There are only two options for the configuration entry: Enable and Disable, where “Enable” enables MSTP while “Disable” disables MSTP. By default, the switch does not enable BPDU monitoring function.

5) Region name

By default, MST region name is the first MAC address of MST region switch. All VLANs in MST region belong to spanning tree instance 0, and the revision level of MSTP region is 0. When the user configures the related parameters of MST region, especially the VLAN distribution table, network topology oscillation can be easily caused. To reduce such oscillation caused by the configuration, MSTP will not immediately trigger the re-calculation of the spanning tree upon processing the related configuration on the region. The configuration of these regions will be valid only when MSTP configuration is enabled.

5.5.2 MSTI Protocol Configuration

I. MSTI information list

Open the device and start MSTP protocol configuration function. The interface shown in Figure 5-6 appears. Select the [MSTI] tab to enter the interface shown in Figure 5-8.

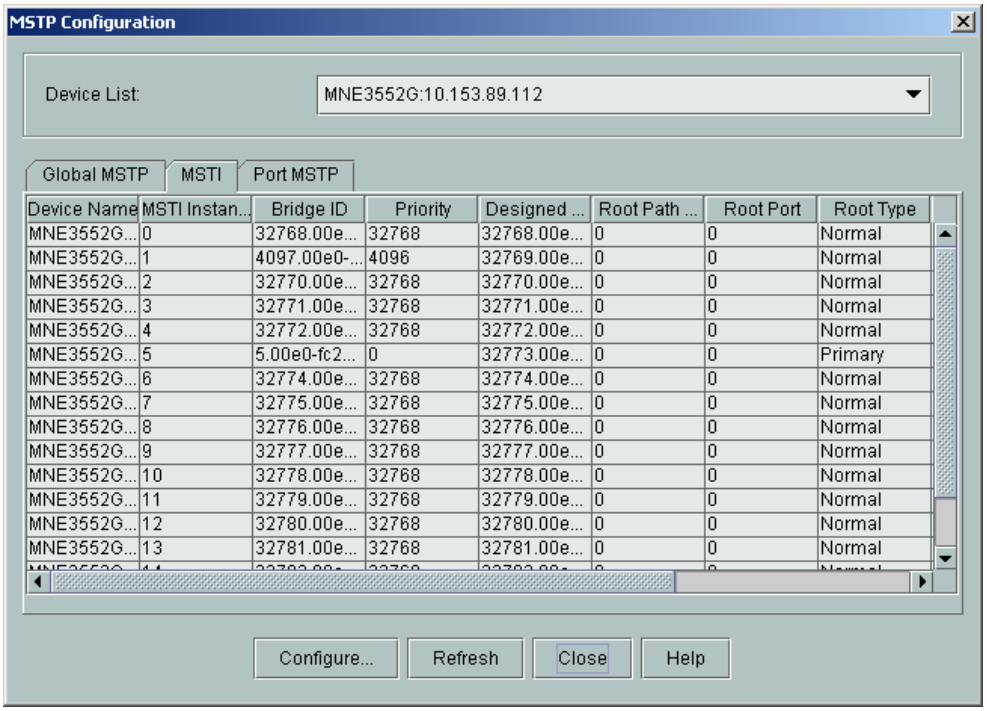


Figure 5-8 MSTI information

II. MSTI configuration

Select one line or multiple lines of data pending for configuration in Figure 5-8, and click <Configure…>. Then, input the appropriate data in the pop-up dialog box, and click <OK> to complete the configuration of MSTI. See Figure 5-9.

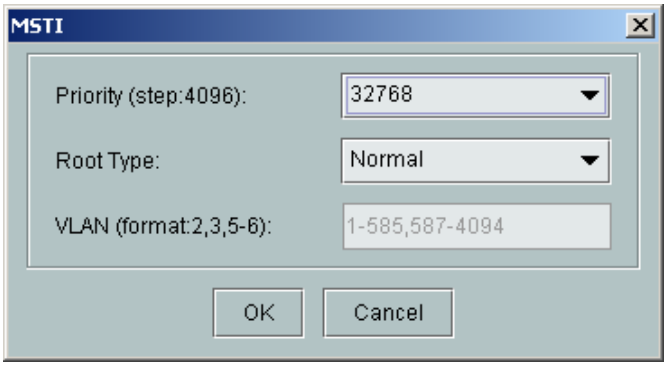


Figure 5-9 MSTI configuration

III. Parameter description

1) Priority

The Bridge priority level of the switch determines whether the switch can be selected as the root of the spanning tree. Configuring low-level Bridge priority can specify a certain switch as the root of the spanning tree. The switch supporting MSTP may have different

priorities in different spanning tree instances. Be fault, the Bridge priority of the switch is 32768.

2) Root Type

Configuring network bridge role is a kind of configuration on the priority, including three options: Normal, Secondary, and Primary. Normal is used for the restoring priority 32768, Primary sets the priority to 0, and Secondary sets the priority to 4096. The lower the priority is, the easier it becomes the root bridge. Be default, it is set to Normal.

3) VLAN

Configured VLAN is used to configure the MST instance corresponding to a certain VLAN. The VLAN distribution list cannot be validated after the configuration is completed before MSTP is enabled.

5.5.3 Port MSTP Protocol Configuration

I. Port MSTP information list

Open the device and start MSTP configuration function. The interface shown in Figure 5-6 appears. Select the [Port MSTP] tab and enter the interface shown in Figure 5-10.

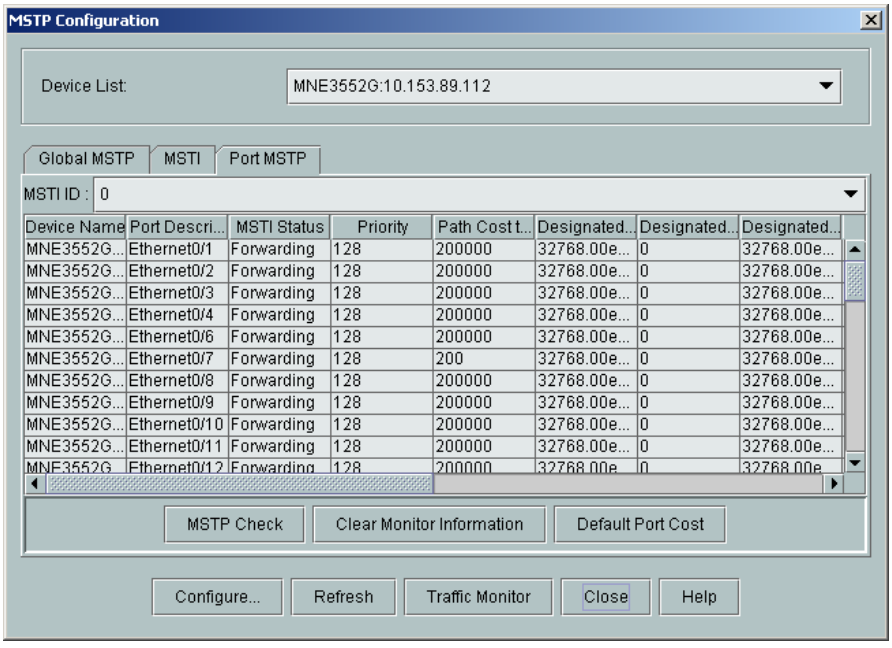


Figure 5-10 Port MSTP information

II. Port MSTP default setting

There are three default configuration buttons for the Port MSTP protocol configuration list as shown in Figure 5-10: <MSTP Check>, <Clear Monitor Information>, and <Default Port cost>.

<MSTP Check> forcefully enters MSTP mode. There are two kinds of operation modes on the switch supporting MSTP: STP compatible mode and MSTP mode. Suppose in a switching network, the switch port running MSTP connects to the switch running STP, and the port will automatically migrate to STP compatible mode to operate. By this time, when the switch running STP is disconnected, the port cannot automatically migrate to MSTP mode, but still operate in STP compatible mode. Setting the mCheck variable may force it to migrate to MSTP mode.

<Clear Monitor Information> clears the MSTP monitoring entry to zero. For details of the port MSTP monitoring entry, refer to the subsequent description.

<Default Port cost> sets the path cost of the port to the default cost.

III. Port MSTP configuration

Select one line or multiple lines of data pending for configuration in Figure 5-10, and click <Configure…>. Then, input the appropriate data in the pop-up dialog box, and click <OK> to complete the configuration on port MSTP. See Figure 5-11.

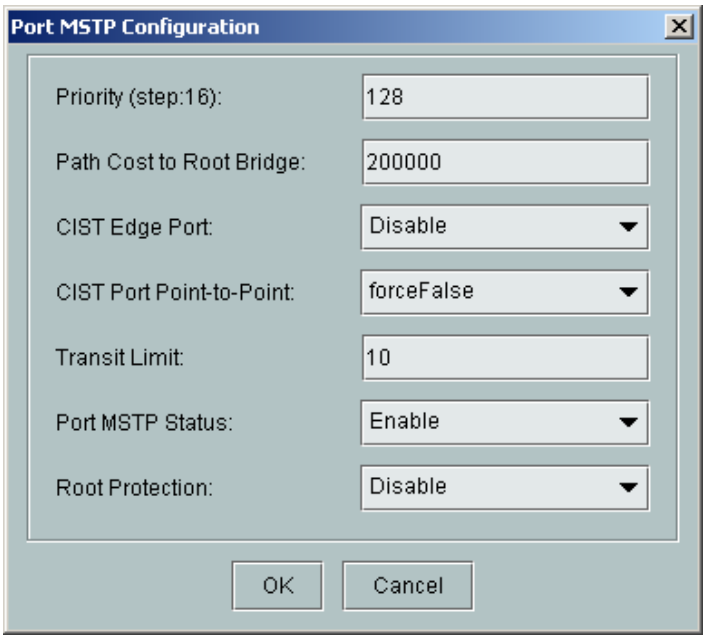


Figure 5-11 Port MSTP Configuration

IV. Parameter description

1) Priority

In the process of calculating the spanning tree, the port priority is the important foundation for whether the port will be selected as the root port. In equal conditions, the port with higher priority will be selected as the root port. On the switch supporting MSTP, the port may have different priorities in different spanning tree instances so that the same port may act varying roles in different spanning tree instances. Thus, data of

different VLANs can be advertised along different physical paths to implement load sharing according to VLAN.

When the port priority changes, MSTP will re-calculate the port role and migrate to the state. Generally, the smaller the configured value is, the higher the port priority is. If all Ethernet ports of the switch adopt the same priority parameter, the priority level of the Ethernet port is determined by the index of the Ethernet port. Changing the priority of the Ethernet port may cause the re-calculation of the spanning tree. The user can set the priority of the port according to the actual requirement of the network.

By default, the priority of all Ethernet ports of the switch is 128.

2) Path Cost to Root Bridge

Root bridge cost to region is the parameter related to the link rate connecting the port. On the switch supporting MSTP, the port may have varying path costs in different spanning tree instances so that traffic of different VLANs can be forwarded along the physical link to complete the load sharing.

By default, MSTP calculates the path cost of each port.

3) CIST Edge Port

It is only applicable to the case when MST instance is CIST. Edge port means that the port is neither directly connected to any switch nor indirectly connected to any switch through the port-connected network. When the user specifies one port as the edge port and when the port migrates from the congestion state to forwarding state, the fast migration can be implemented without waiting for delay time. The user can only set the port connecting the terminal to the edge port. If BPDU packet from other port is received on the edge port, the port will become the non-edge port again. The parameter is valid for all spanning tree instances, meaning that when the port is configured as the edge port or non-edge port, the port is set as the edge port or non-edge port on CIST and all MSTI.

When the port receives BPDU, the actual operation value is also the non-edge port even it is set as the edge port by the user.

By default, all Ethernet ports of the switch are configured as the non-edge ports.

4) CIST Port Point-to-Point

Point-to-Point link generally refers to the link between switches. The two ports in point-to-point link can be quickly migrated to forwarding state by transmitting the synchronous packets, in which way the forwarding delay is reduced. If the parameter is configured as the automatic mode, MSTP can automatically detect whether the current Ethernet port is the point-to-point link. It must be noted that for aggregation port only the primary port of the aggregation port can be configured as the point-to-point link. When one port operates in the auto-negotiation mode and the negotiated operation mode is the full duplex mode, the port can be configured as the point-to-point link.

The configuration is valid for CIST and all MSTI. When the port is set to point-to-point link or non-point-to-point, the port is set to point-to-point link or non-point-to-point on all spanning tree instances. If the actual physical link of the port is not the point-to-point link and the user wrongly configures it as forced point-to-point link, the temporary loop may be redistributed.

By default, the parameter is set to auto.

5) Transit Limit

It is the configuration of the maximum forwarding rate. It is related to the physical state and the network structure of the port, and the user can configure as required.

It must be noted that if the larger the parameter is configured, the more the packets are sent per unit time, consequently occupying more network resources. The default is recommended.

By default, the maximum transmission rate for all Ethernet ports on the switch is 3 (it is the value of the counter, and no unit is assigned to it).

6) Port MSTP Status

To flexibly control MSTP, the user can disable the specified MSTP feature on the switch Ethernet port so that these ports will not participate in the calculation of the spanning tree, saving the CPU resources of the switch.

By default, the MSTP feature on all ports is enabled.

7) Root Protection

The root switch and backup switch of the spanning tree shall be within the same region, especially the root switch and backup switch of CIST. Generally, the root switch and backup switch of CIST will be placed in the core region of high-bandwidth upon network design. Sometimes, due to the error configuration by the maintenance staff or vicious attack by the user, the valid root switch of current root switch may receive the configuration message of higher priority, in which way the current root switch loses its status as the root switch and causes the error change of the network topology structure. Such invalid change may cause the traffic, which shall pass the high-speed link, to be pulled to the low-speed link, resulting in network congestion. Root monitoring function may prevent such case.

For port configured with Root monitoring function, the port role on all instances can only be the specified port. Once such port receives the configuration message with higher priority, meaning that it is selected as the non-specified port, the state of these ports will be set as the snooping state and no packet will be forwarded (equivalent to disconnecting the link connecting the port). When the priority of the received configuration message is lower than that of the local configuration message, the port will automatically migrate from the snooping state, via the transit state, to the normal forwarding state.

By default, the switch does not enable ROOT monitoring function.

V. Port MSTP traffic monitoring

When it is switched to the [Port MSTP] tab, <Traffic Monitor> appears in the command button area of the protocol management window. Select a certain line of port information, and click the button to enter the port MSTP traffic monitoring window. See Figure 5-12.

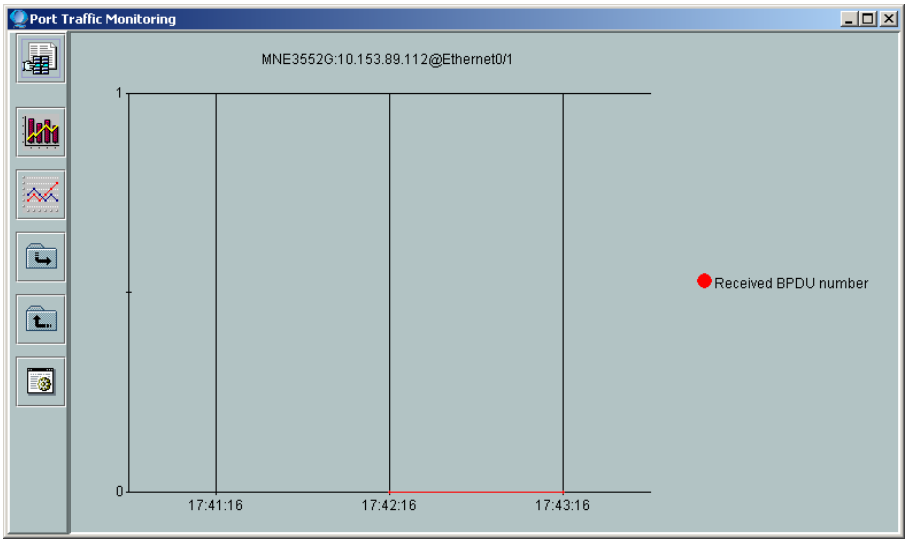


Figure 5-12 Port traffic monitoring

Click in Figure 5-12, and the system pops up the [Select Items to Be Monitored] dialog box. Select one or multiple monitoring entries in the window for monitoring.

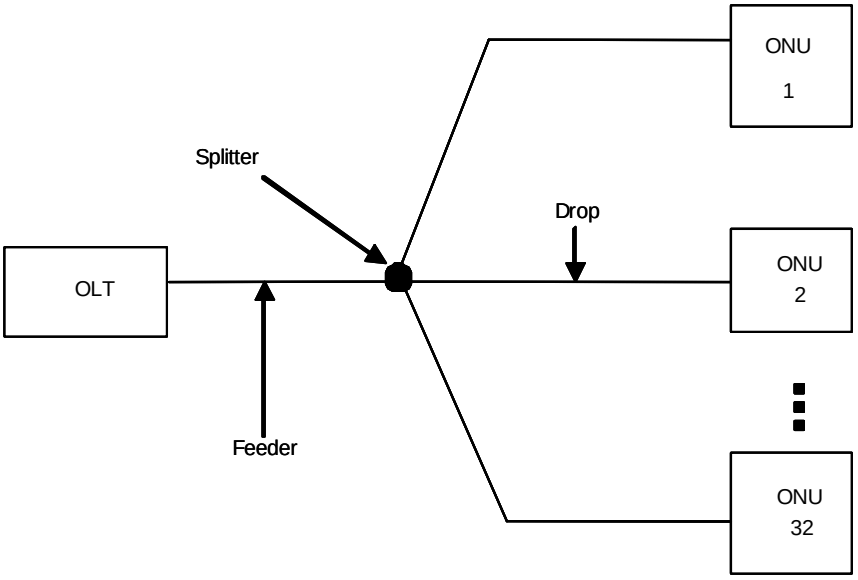
MSTP monitoring entry includes the received BPDU packets, received TCN BPDU packets, sent TCN BPDU packets, received RST BPDU packets, sent RST BPDU packets, received MST BPDU packets, and send MST BPDU packets.

Chapter 6 EPON Management

6.1 Overview

As a kind of passive optical network (PON) technology, the Ethernet passive optical network (EPON) currently ranks high among all fiber to the home (FTTH) solutions. The emergence of 10 Gbps Ethernet backbone and metropolitan area network (MAN) will make EPON the best last-mile solution in all-optical network in the future.

The IEEE 802.3ah standard details the operation model of the EPON, including multiple point control protocol (MPCP) and operation, administration and maintenance (OAM) functions. Figure 6-1 illustrates the EPON system architecture.



Splitter Drop: Data downlink
Feeder: Data are multiplexed into one fiber

Figure 6-1 EPON system architecture

A typical EPON system consists of optical line terminal (OLT), optical network unit (ONU) and passive optical splitter (POS).

- OLT provides a platform for multiple services and serves as an interface between the EPON system and the core data, video and telephone network of the service providers. Currently, S6500 series Ethernet switches with service cards concerning EPON features installed are used as the OLT devices and placed in the central office (CO).
- The ONUs are placed near the network interface units (NIUs) or integrated with the NIUs.

- The POS connects the OLT and the ONUs, and consists of a trunk port and multiple branch ports. It can operate in an all-weather environment. In the downlink direction, the POS distributes the incoming optical signals through multiple outgoing ports, and thus multiple users can share the bandwidth by using only one fiber; in the uplink direction, the POS multiplexes multiple ONU optical signals into one fiber.

The data transmission procedures of an EPON system are as follows:

- In an EPON system, the downlink data (packets sent from OLT to ONUs), are broadcasted to every ONU. An ONU receives packets of its own logical link identifier (LLID) or the broadcast LLID, and forwards them to each port.

Note:

- LLID refers to the value that the OLT assigns to an ONU dynamically, and it can identify an ONU uniquely.
- Currently, LLID ranges from 1 to 32.

- In the uplink direction, packets are time-division multiplexed from ONUs to the OLT. OLT assigns a slot to each ONU, and each ONU takes its turn one by one to send packets without interfering each other.
- The POS couples the uplink data to an optical fiber and distributes the downlink data to each ONU.
- To avoid data collisions and implement signal synchronization, automatic ranging between the OLT and ONUs are required, and the uplink bandwidth must be allocated based on the service level agreement (SLA) of each user.

An EPON system features the following:

1) Point-to-multipoint architecture

One OLT port can connect to up to 32 ONUs (expandable in the future); all ONUs of an OLT port can share an uplink bandwidth of up to 1 Gbps through time division multiplexing (TDM).

2) Passive optical fiber transmission

Without the help of any complex protocol, EPON ensures that optical signals are transmitted to end users correctly, and the data from end users are centralized and transmitted to the core network.

3) Ethernet-based network architecture

EPON adopts IP/Ethernet architecture, which is used by more than 95% of the whole LAN at present. Thus, EPON becomes one of the most effective communication methods for the end users accessing the network.

Intended for management on EPON features, Device Manager provides the following functions:

- EPON system management
- EPON OLT management
- EPON ONU management
- EPON batch operations
- EPON OAM management
- EPON device management

All these functions are introduced elaborately below.

⚠ **Caution:**

The ranges and default values for part of the parameters involved in this section vary depending on the device versions. The descriptions in this chapter are only for reference. See related device manuals for more details.

6.2 EPON System Management

Enable Device Manager first. On the Functions navigation tree, click “+” on the “EPON Management” node, and then double-click the extended leaf node “EPON System Management” to enter the [EPON System Management] dialog box shown in Figure 6-2.

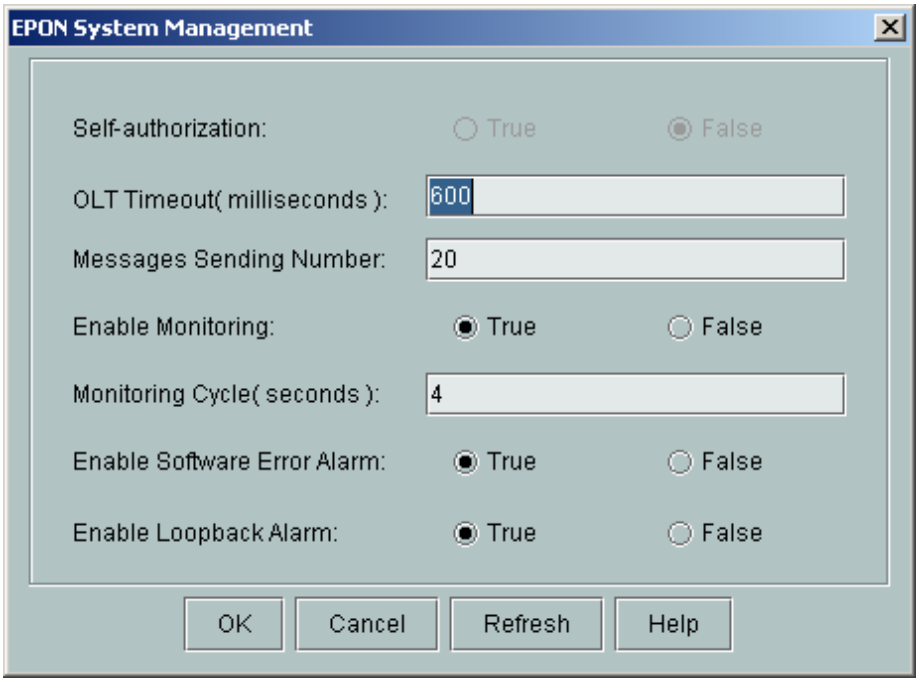


Figure 6-2 EPON System Management

This dialog box allows you to implement EPON system configuration and management. You can confirm or cancel the configurations on EPON system parameters through the buttons at the bottom of the interface.

The involved parameters on the [EPON System Management] dialog box and their meanings are shown in Table 6-1.

Table 6-1 Descriptions on the EPON system management parameters

Parameter	Description
Self-authorization	Indicates whether to enable automatic authorization on ONU devices. True indicates that automatic authorization is enabled, while False indicates disabled.
OLT Timeout (milliseconds)	Indicates the message timeout between the HOST (CPU of the LPU with EPON function in the OLT) and the OLT device. That is, the timeout of waiting for the response messages from OLT.
Message Sending Number	Indicates the message timeout times between the HOST and the OLT. When the times reach the defined value, the OLT will be reset.
Enable Monitoring	Indicates whether to enable the alarm monitor of the EPON system. You can select True (enable) or False (disable).
Monitoring Cycle (seconds)	Indicates the alarm monitoring period.

Parameter	Description
Enable Software Error Alarm	Indicates whether to enable the software error alarm. You can select True (enable) or False (disable). If it is enabled, the system generates a software error alarm when a signal error, DA abnormity (that is, data inconsistency), or memory allocation failure occurs.
Enable Loopback Alarm	Indicates whether to enable the loopback alarm of the EPON system. When a loopback occurs between two sub-ports of one ONU or two ONUs connected to the OLT, a loopback alarm is generated. You can select True (enable) or False (disable).

Note:

- If automatic authorization is used, the ONU automatically registers to join the EPON system once the ONU is powered on. The ONU and the OLT can exchange data without manually binding the ONU port and ONU MAC address. This method is vulnerable to security problems, so the device does not support automatic authentication currently.
- If non-automatic authorization is used, the EPON system will let all ONUs register successfully. The ONU and OLT can exchange data after the ONU port and ONU MAC address is manually bound.

6.3 EPON OLT Management

S6500 series Ethernet switches with service cards concerning EPON features installed can be used as the OLT devices. The OLT device is a platform to provide multiple services, and it can be connected to such devices as voice gateways and IP routers. Besides, it can provide multiple 1000M Ethernet interfaces, and the switching and routing functions at layer 2 and layer 3.

Device Manager implements the management on system information, DBA algorithm, OLT primary status and alarm threshold of OLT devices.

6.3.1 OLT System Information

This function is used to view and define OLT system parameters.

On the Functions navigation tree, click “+” on the “EPON Management” node, and then double-click the extended leaf node “EPON System Management” to enter the [EPON OLT Management] dialog box. Select the [OLT System Information] tab to enter the [OLT System Information] page, as shown in Figure 6-3.

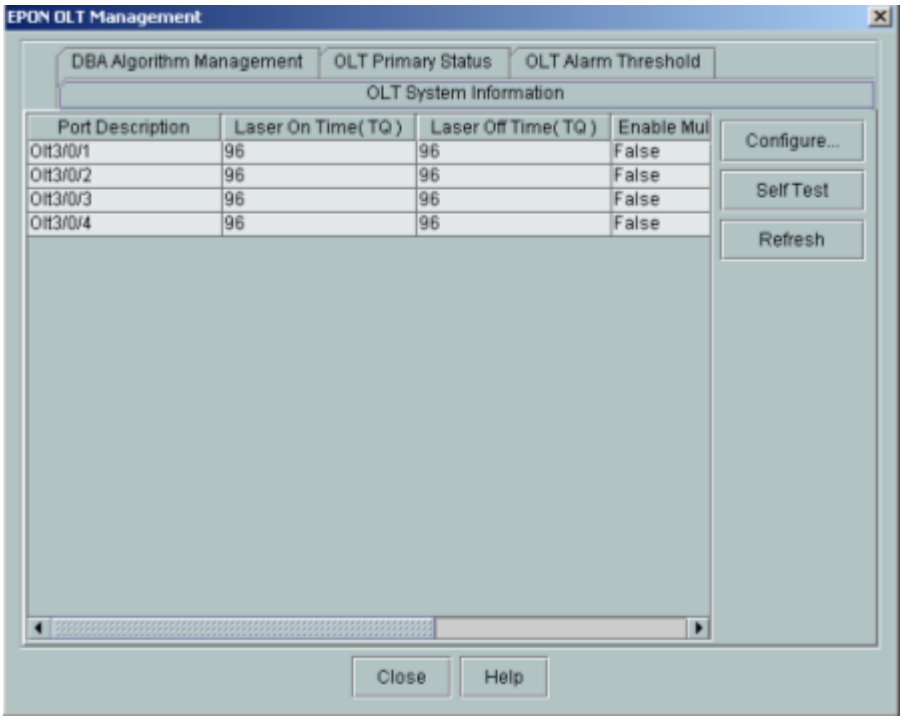


Figure 6-3 OLT System Information

The descriptions on the main parameters involved on this interface are shown in Table 6-2.

Table 6-2 Descriptions on OLT system information parameters

Parameter	Description
Port Description	Descriptions on the OLT device.
Laser On Time (TQ)	The open time period of an OLT laser in the discovery stage starts from the opening of the OLT laser and ends until the laser reaches the stable active state.
Laser Off Time (TQ)	The close time period of an OLT laser in the discovery stage starts from the closing of the OLT laser and ends until the laser reaches the stable inactive state.
Enable Multicast	If the multicast copy broadcast is enabled, when the OLT device forwards a packet to an ONU, the same packet is broadcasted in the VLAN that the packet belongs to instead of in all VLANs.
Enable Discard Packet	Indicates whether or not the system discards the packets whose source MAC addresses are not contained in the OLT MAC address table.
Latest Self Test Result	Indicates whether the last self test succeeds or not.

You can select the OLT to be configured on the [OLT System Information] page, and click <Configure…> to open the [OLT System Parameters Configuration] dialog box, where you can configure related system information parameters.

You can select the OLT to be tested and click <Self Test> to enable the self test.

Note:

- The discovery stage is a stage when the OLT discovers and registers the ONUs and assigns bandwidth to the ONUs.
- Currently, multiple copy broadcast is not supported.
- Some above configurations can take effect only when the OLT is opened again after it is closed.
- 1 TQ is equal to 16 nanoseconds (ns).

6.3.2 DBA Algorithm Management

The dynamic bandwidth allocation (DBA) feature can adjust the uplink bandwidth of an ONU in real time according to the immediate service state of ONUs.

DBA can be implemented by adopting the request/response mechanism. Flow information about each ONU is collected by receiving bandwidth requests from the ONUs. The system invokes the corresponding bandwidth allocation algorithm to figure out the bandwidth to be allocated to each ONU and notifies each ONU through bandwidth authorization messages. This ensures these ONUs do not conflict with each other when they transmit uplink packets.

Compared with fixed bandwidth allocation schemes, DBA is more suitable for IP/Ethernet services with large burst flow. DBA helps to reduce wasted bandwidth and utilize uplink bandwidth more efficiently. The ONUs take their turns one by one to send uplink packets. The transmitting order and the time are controlled by OLT.

Note:

- In the discovery stage, OLT is active and ONU is passive. OLT broadcasts its discovery requests, and ONUs respond the requests preemptively.
- DBA is only available to uplink packets.

In the [EPON OLT Management] dialog box, select the [DBA Algorithm Management] tab to enter the [DBA Algorithm Management] page, as shown in Figure 6-4.

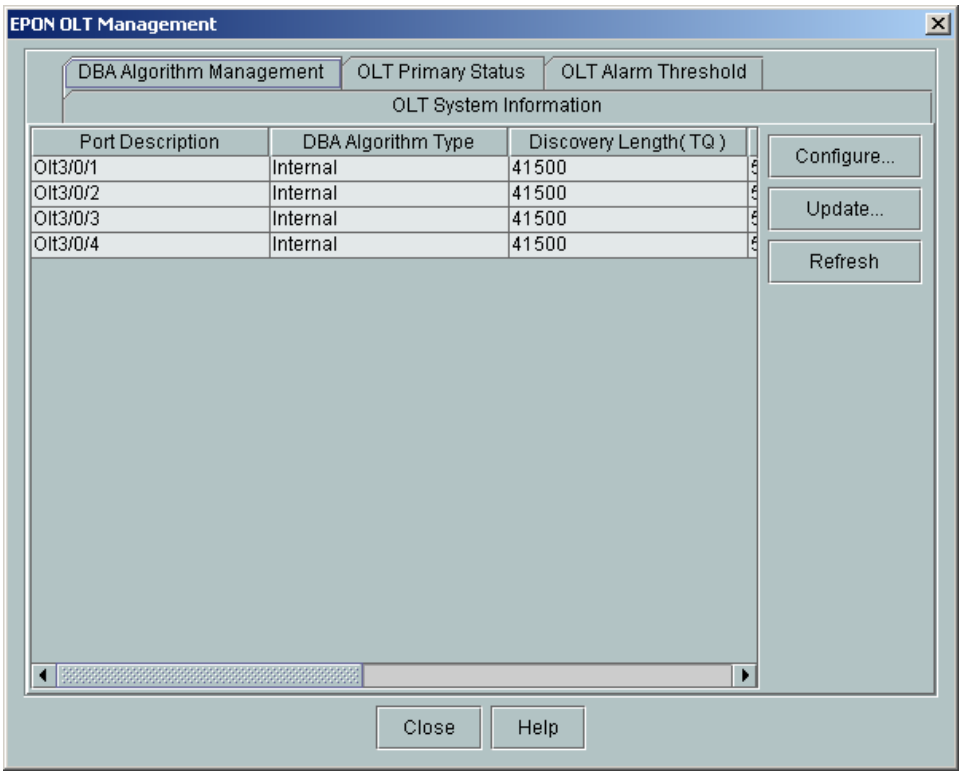


Figure 6-4 DBA Algorithm Management

The descriptions on the main parameters involved on this interface are shown in Table 6-3.

Table 6-3 Descriptions on DBA algorithm parameters

Parameter	Description
DBA Algorithm Type	Indicates the type of the adopted DBA algorithm. By default, the internal DBA algorithm is adopted.
Discovery Length (TQ)	Specifies the period in TQs for the OLT to discover the ONUs.
Discovery Frame frequency	Specifies the frequency for the OLT to send discovery frames to the ONUs based on the grant cycle (measured in cycle-lengths). It ranges from 25 to 100 and defaults to 50. For example, if you set the frequency to 30, the OLT sends discovery frames to the ONUs in every period 30 times of the cycle-lengths.
Cycle Length (TQ)	Specifies the cycle-length in TQs (grant cycle is measured in cycle-lengths).
DBA Version	Specifies the used DBA version.
Latest Update Result	Specifies the latest update result of the DBA algorithm.

You can select the OLT to be configured on the [DBA Algorithm Management] page and click <Configure...> to enter the [DBA Parameters Configuration] dialog box, where you can configure related parameters.

You can also update the DBA algorithms on some OLT ports simultaneously. Select some OLT whose software needs update on the [DBA Algorithm Management] page and click <Update…> to open the [Software Updating] dialog box. Select a new algorithm file from the Update File Name drop-down list and click <OK>. If the update file has not been uploaded to the device, you can click to enter the [Upload Tool] dialog box, where you can perform related operations to upload the file to the device.

6.3.3 OLT Primary Status

This function is mainly used to view the OLT status information. On the [EPON OLT Management] dialog box, select the [OLT Primary Status] tab to enter the [OLT Primary Status] page, where you can view the OLT status information. The main parameters and their meanings are shown in Table 6-4.

Table 6-4 Descriptions on main OLT status parameters

Parameter	Description
Software Major Version	Software major version of the OLT
Software Minor Version	Software minor version of the OLT
Hardware Major Version	Hardware major version of the OLT
Hardware Minor Version	Hardware minor version of the OLT
AGC Lock Time (TQ)	Automatic gain control (AGC) time is the time period during which the receivable signal strength is restored automatically.
RX Signal Synchronization Time (TQ)	CDR time is used to recover clock data.
UNI Mac Address	OLT MAC address.
Operation Mode	OLT status.

6.3.4 OLT Alarm Configuration

On the [EPON OLT Management] dialog box, select the [OLT Alarm Threshold] tab to enter the [OLT Alarm Threshold] page, as shown in Figure 6-5.

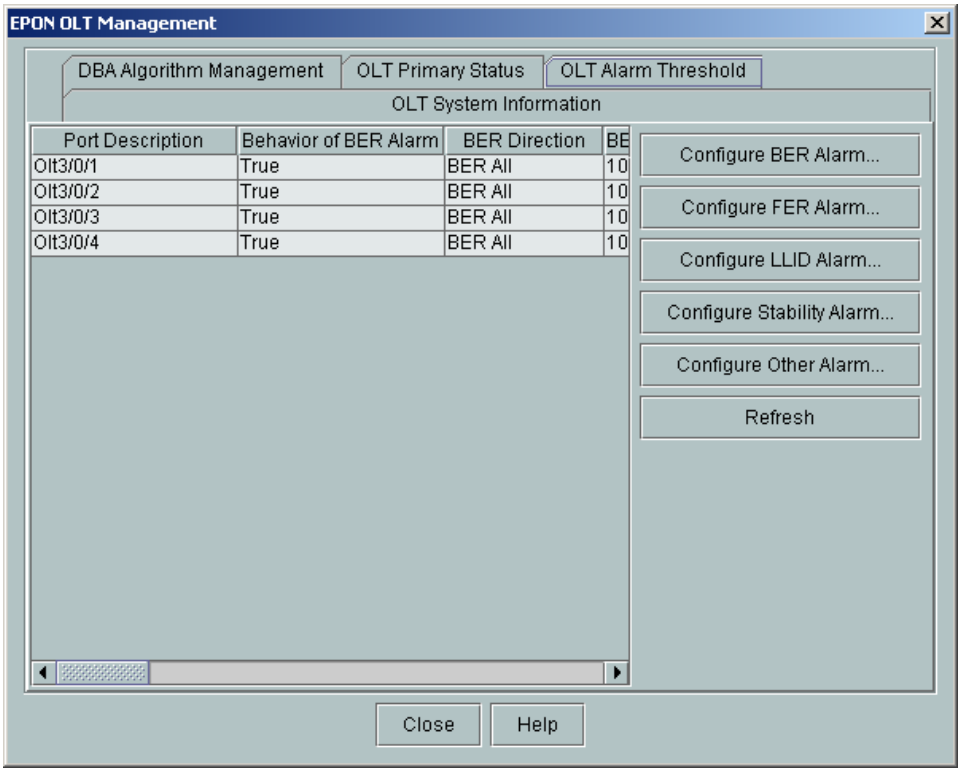


Figure 6-5 OLT Alarm Threshold

The descriptions on the main parameters involved on this interface are shown in Table 6-5.

Table 6-5 Descriptions on OLT alarm parameters

Parameter	Description
Behavior of BER Alarm	Indicates whether to enable the bit error rate (BER) alarm. The system generates a bit error rate alarm when an optical path between ONU and OLT is abnormal due to out-of-range optical path attenuation or improper configuration of ONU or OLT optical parameters. By default, this function is enabled, and both uplink and downlink data between OLT and ONU are monitored.
BER Direction	Indicates the monitor direction. It can be Uplink, Downlink, or All. Uplink indicates that only the uplink data forwarded from ONU to OLT are monitored; Downlink indicates that only the downlink data forwarded from OLT to ONU are monitored; All indicates that both the uplink and downlink data transmitted between OLT and ONU are monitored.
BER Threshold (1E–9)	Indicates the BER alarm threshold (the order of magnitude is 10^{-9}).

Parameter	Description
Behavior of FER Alarm	Indicates whether to enable frame error rate (FER) alarm. The system generates a frame error rate alarm when an optical path between ONU and OLT is abnormal due to out-of-range optical path attenuation or improper configuration of ONU or OLT optical parameters. By default, this function is enabled, and both uplink and downlink data between OLT and ONU are monitored.
FER Direction	Indicates the monitor direction. It can be Uplink, Downlink, or All. Uplink indicates that only the uplink data forwarded from ONU to OLT are monitored; Downlink indicates that only the downlink data forwarded from OLT to ONU are monitored; All indicates that both the uplink and downlink data transmitted between OLT and ONU are monitored.
FER Threshold (1E–9)	Indicates the alarm threshold of the frame error rate (the order of magnitude is 10^{-9}).
Enable LLID Mismatch Alarm	Indicates whether to enable the LLID mismatch frame alarm. The system generates an LLID mismatch frame alarm when the slots are used in disorder, that is, one ONU uses another ONU's slot to forward data. By default, this function is disabled.
Threshold of LLID Alarm	Specifies the alarm threshold of LLID mismatch frame. It ranges from 1,000 to 10^9 and defaults to 5,000. Its unit is frames-per-second.
Enable OLT Remote Stability Alarm	Indicates whether to enable the remote mismatch alarm. The system generates a remote mismatch alarm when system misuse occurs, for example, an OAM 1.2 ONU and an OAM 2.0 ONU are mixed in the same system. (All ONUs in the same system must adopt the same OAM version.)
Enable OLT Local Stability Alarm	Indicates whether to enable the local mismatch alarm. The system generates a local mismatch alarm when system misuse occurs, for example, an OAM1.2 ONU and an OAM2.0 ONU are mixed in the same system. (All ONUs in the same system must adopt the same OAM version.)
Enable Registration Alarm	Indicates whether to enable the registration error alarm. The system generates a registration error alarm when an error occurs during the registration of an ONU.
Enable OAM Disconnection Alarm	Indicates whether to enable the OAM link disconnection alarm. The system generates an OAM link disconnection alarm when OAM link is disconnected.
Enable Encryption Key Alarm	Indicates whether to enable the bad encryption key alarm. The system generates a bad encryption key alarm when you change the encryption key which should not be changed.
Enable Vendor Specific Alarm	Indicates whether to enable the OAM vendor specific alarm. This alarm is customized by vendors.

You can select the OLT to be configured and click the buttons on the right side to open the corresponding dialog boxes to configure related alarms.

6.4 EPON ONU Management

ONU devices are used by users, and provide interfaces for users to connect to PON through Ethernet. ONU devices translate optical signals received from OLT into Ethernet packets and transfer them to users. They also translate the Ethernet packets received from users into optical signals and transfer them to OLT.

Device Manager implements management on system information, downstream bandwidth and upstream bandwidth of ONU.

Enable Device Manager first. On the Functions navigation tree, click “+” on the “EPON Management” node, and then double-click the extended leaf node “EPON ONU Management” to enter the [EPON ONU Management] dialog box.

6.4.1 ONU System Information

On the [EPON ONU Management] dialog box, select the [ONU System Information] tab to enter the [ONU System Information] page, as shown in Figure 6-6.

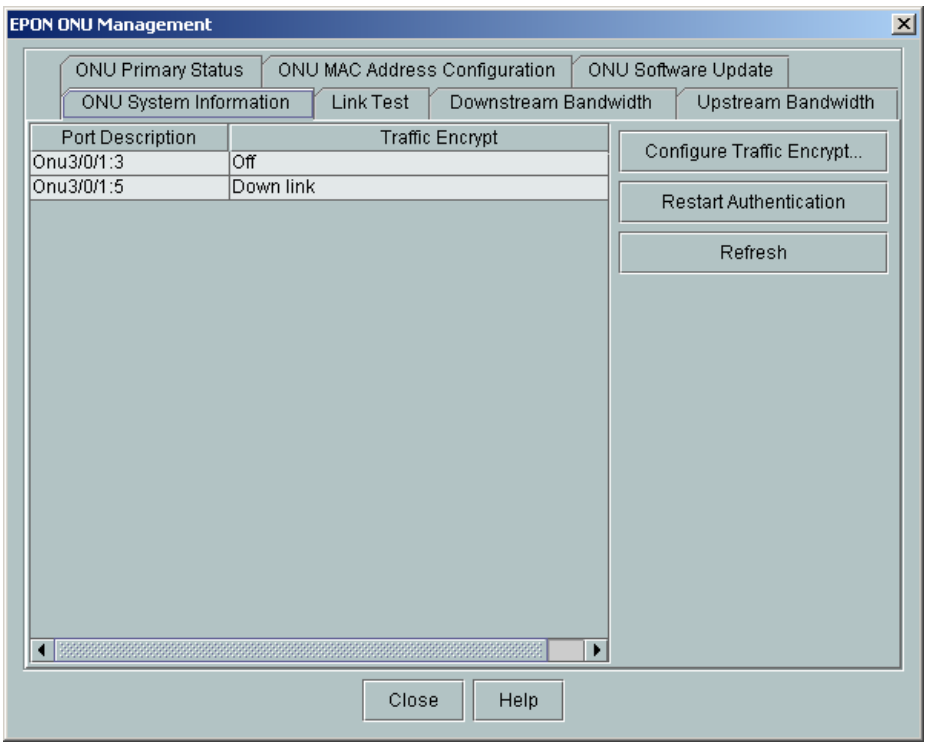


Figure 6-6 ONU System Information

The traffic encryption configurations are displayed. You can select the ONU to be configured, and click <Configure Traffic Encrypt…> to open the [ONU System Parameters Configuration] dialog box, where you can configure traffic encryption. The traffic encryption falls into three types:

off: Indicates that the encryption function is disabled.

downlink: Indicates that only the data which is sent from the OLT to the ONU are encrypted.

up-down-link: Indicates that both the uplink and downlink data between the OLT and the ONU are encrypted.

By default, only the data sent from the OLT to the ONU are encrypted.

To prevent your data from being accessed by unauthorized users, you can encrypt your data by using encryption algorithms. To ensure data security, it is strongly recommended that downstream data, which is sent from OLT to ONU, be encrypted.

You can also click <Restart Authentication> to re-authenticate ONU forcibly.

6.4.2 Link Test Management

The link test function is used to test whether the link between an ONU and the OLT is in normal state.

On the [EPON ONU Management] dialog box, select the [Link Test] tab to enter the [Link Test] page. Select the link to be tested, and click <Test…> to enter the [ONU Link Test Parameters Configuration] dialog box. Input proper test parameters, and then click <OK> to test the selected link.

Table 6-6 Descriptions on the link test main parameters

Parameter	Description
Number of Test Frames	It ranges from 1 to 250.
Frames Data Times	It ranges from 60 bytes to 1514 bytes.
Enable Delay Test	Indicates whether or not to enable delay test. True indicates enabling delay test. False indicates disabling delay test.
Enable VLAN Tag	True indicates using the frames with VLAN tag to perform test. False indicates not using the frames with VLAN tag to perform test.
VLAN Priority	It ranges from 0 to 7. The bigger the value is, the higher the priority is.
VLAN Tag ID	It ranges from 1 to 4094.

Caution:

- Only when ONU is online (that is, ONU is UP) can it be tested.
- Before these configurations, the system needs to bind the ONU and the ONU port.

6.4.3 Downstream Bandwidth Management

The downlink bandwidth management is used to allocate static downstream bandwidth for an ONU. The EPON system can allocate bandwidth according to service requirements of clients. You can allocate higher bandwidth for medium- and large-sized enterprises to allow for their services and limit the bandwidth allocated for individuals to avoid wasting bandwidth resources.

On the [EPON ONU Management] dialog box, select the [Downstream Bandwidth] tab to enter the [Downstream Bandwidth] page, where you can view the current bandwidth configuration status. Select the ONU to be configured, and click <Configure…> to open the [ONU Downstream Bandwidth Parameters Configuration] dialog box, as shown in Figure 6-7. After configuring proper parameters, click <OK>.

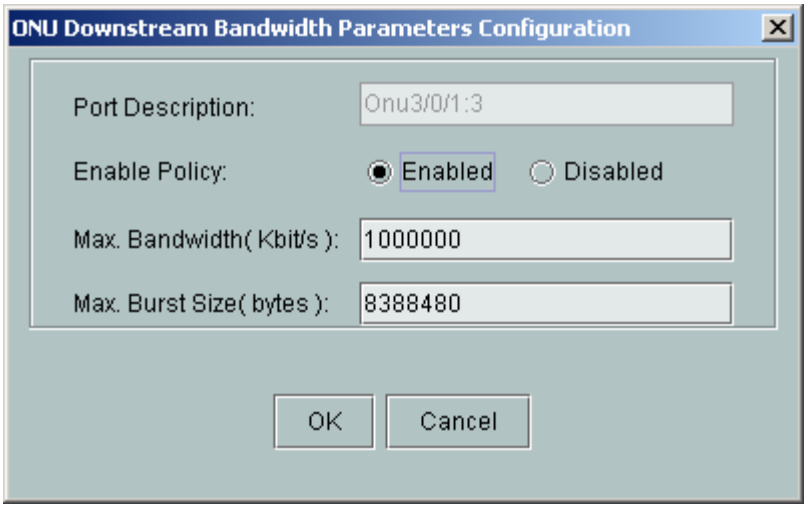


Figure 6-7 ONU Downstream Bandwidth Parameters Configuration

The main parameters involved on this dialog box and their meanings are shown Table 6-7.

Table 6-7 Descriptions on bandwidth management parameters

Parameter	Description
Enable Policy	Disabled means that the bandwidth allocation policy is disabled, while Enabled means that the bandwidth allocation policy is enabled. By default, the downstream bandwidth allocation policy is enabled.
Max. Bandwidth (Kbit/s)	It ranges from 0 to 1,000,000 with the unit of kbps.
Max. Burst Size (bytes)	It ranges from 0 to 8,388,480 with the unit of bytes.

Caution:

- These configurations take effect only if ONU is in UP state.
- Before these configurations, you need to bind the ONU and the ONU port first.
- The configurations of parameters concerning bandwidth allocation can take effect only when the bandwidth allocation policy is enabled.

6.4.4 ONU MAC Address Configuration

This function is used to bind an ONU port to the MAC address of an ONU, thus allowing the OLT and the ONU to communicate with each other, and the OLT to manage the ONU.

On the [EPON ONU Management] dialog box, select the [ONU MAC Address Configuration] tab to enter the [ONU MAC Address Configuration] page, where you can view the current address binding information. Select the ONU port to be configured, and click <Configure MAC Address…> to open the [ONU MAC Address Configuration] dialog box. After selecting the MAC address to be bound, click <OK>.

You can also select an ONU port and click <Undo Bind> to remove the binding relationship.

6.4.5 Upstream Bandwidth Management

The upstream bandwidth management refers to configuring the upstream maximum and minimum bandwidth of an ONU (the bandwidth is allocated dynamically with the DBA algorithm according to the immediate service status of each ONU).

On the [EPON ONU Management] dialog box, select the [Upstream Bandwidth] tab to enter the [Upstream Bandwidth] page, where you can view the current upstream bandwidth configuration. Select the ONU to be configured, and click <Configure…> to open the [ONU Upstream Bandwidth Parameters Configuration] dialog box. After configuring proper parameters, click <OK>.

Caution:

- The above configurations take effect only if the ONU is in UP state.
- Before these configurations, you should first bind the ONU and the ONU port.
- The order of magnitude for the upstream bandwidth is 500 kbps.
- To prevent the internal DBA algorithm from losing effect, make sure that the total minimum bandwidth of all ONUs connected to an OLT port does not exceed 1,000,000 kbps.

6.4.6 ONU Primary Status

This function is used to display such information of an ONU as the hardware and software version, laser on time, laser off time and grant FIFO depth during ONU authorization.

6.4.7 ONU Software Update

This function is used to update the software of some ONU. On the [EPON ONU Management] dialog box, select the [ONU Software Update] tab to enter [ONU Software Update] page. Select the ONU whose software needs update, and click <Update…> to open the [Software Updating] dialog box. Select an update file and click <OK>. If you cannot find the desired file, click to enter the [Update Tool] dialog box, where you can configure related parameters to upload the file to the device.

6.4.8 ONU Packet Management

This function is used to configure the UNI queue scheduler algorithm and priority used for queue scheduler on the ONU.

In the [EPON ONU Management] dialog box, select the [ONU Packet] tab.

Table 6-8 lists the parameters in the [ONU Packet] tab and their meanings.

Table 6-8 Description on ONU packet management parameters

Parameter	Description
Priority Trust	There are three priority trust modes: • DSCP: Put the packets into the port export queue according to the DSCP priority. The DSCP priority ranges from 0 to 63. If the priority of the packet is between 0 and 7, put the packet into queue 0. If the priority of the packet is between 8 and 15, put the packet into queue 1, and so on. • IP-precedence: Put the packets into the port export queue according to the IP-precedence. The IP-precedence ranges from 0 to 7. If the priority of the packet is 0, put the packet into queue 0. If the priority of the packet is 1, put the packet into queue 1, and so on. • CoS: Put the packets into the port export queue according to the 802.1p priority. The 802.1p priority ranges from 0 to 7. If the priority of the packet is 0, put the packet into queue 2. If the priority of the packet is 1, put the packet into queue 0. If the priority of the packet is 2, put the packet into queue 1. For the rest packets, the queue number is the same with the priority of the packet.
Queue Scheduler	There are two queue schedulers: • Strict Priority Queuing (SPQ): It can ensure the bandwidth and delay of high-priority queues. • Weighted Fair Queuing (WFQ): It is a complicate queuing process. Only simple configuration is required to dynamically test the communication streams between applications and automatically manage the independent packets for these streams.

After selecting the ONU to be configured, you can click <Configure…> to set the related parameters in the pop-up [ONU Packet Configuration] dialog box.

6.4.9 ONU Protocol Management

This function is used to configure the UNI protocol, including STP, IGMP Snooping, and DHCP Snooping.

In the [EPON ONU Management] dialog box, select the [ONU Protocol] tab.

Table 6-9 lists the parameters in the [ONU Protocol] tab and their meanings.

Table 6-9 Description of ONU protocol management parameters

Parameter	Description
STP Status	Status of the Spanning Tree Protocol (STP). Two statuses are available: Enabled and Disabled.
IGMP Snooping Status	Status of the IGMP Snooping. Two statuses are available: Enabled and Disabled.

Parameter	Description
DHCP Snooping Status	Status of the DHCP Snooping. Two statuses are available: Enabled and Disabled.

After selecting the ONU to be configured, you can click <Configure…> to set the related parameters in the pop-up [ONU Protocol Configuration] dialog box.

6.4.10 ONU dot1x Authentication

This function is used to set the ONU dot1x account and password.

In the [EPON ONU Management] dialog box, click.

Table 6-10 lists the parameters in the [ONU dot1x] tab and their meanings.

Table 6-10 Description of ONU dot1x authentication parameters

Parameter	Description
Account	Account used for the 802.1x authentication of ONU. It is a string with 1 to 16 characters.
Password	Password used for the 802.1x authentication of ONU. It is a string with 1 to 16 characters.

After selecting the ONU to be configured, you can click <Configure…> to modify the account and password in the pop-up [ONU dot1x Configuration] dialog box.

Caution:

- The time spent to write the account and password into the EEPROM of ONU varies with their lengths. The longest time spent is about 20 seconds. Therefore, you are recommended not to power on or off the ONU during the configuration of 802.1x account and password to avoid data written errors.
- The account cannot be set to “a”, “al”, “all”, or the capitalized ones.

6.5 EPON Batch Operation

This function allows you to update the OLT DBA software or ONU software by slot, and update the ONU software by OLT.

6.5.1 Batch Operation by Slot

This function is used to update the software of all OLTs on the LPU with EPON functions in a certain slot or update the software of all connected ONUs.

On the Functions navigation tree, click "+" on the "EPON Management" node, and then double-click the extended leaf node "EPON Batch Operation" to enter the [EPON Batch Operation Management] dialog box. Select the [Batch Operation by Slot] tab to enter the [Batch Operation by Slot] page, as shown in Figure 6-8.

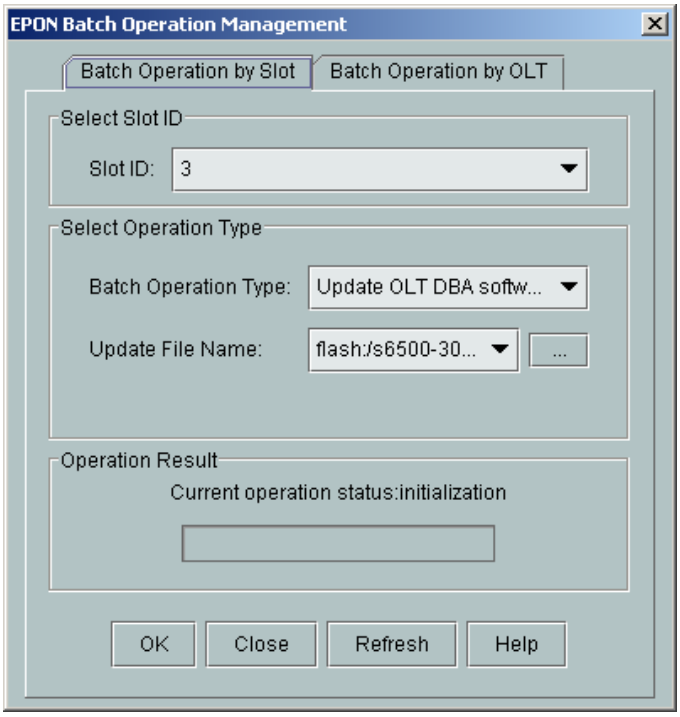


Figure 6-8 Batch Operation by Slot

Select the slot where the LPU with OLT to be updated is located, select the batch operation type (Update OLT DBA Software or Update ONU Software) and the corresponding update file, and then click <OK>. If the desired file is not found, you can click to upload the file to the device.

6.5.2 Batch Operation by OLT

This function is used to update the software of all ONUs connected to a certain OLT port. On the [EPON Batch Operation Management] dialog box, select the [Batch Operation by OLT] tab to enter the [Batch Operation by OLT] page. Select the OLT whose connected ONUs you need to update, select the batch operation type (Update ONU Software) and the corresponding file, and then click <OK>. If the desired file is not found, you can click to upload the file to the device.

6.6 EPON OAM Management

This function enables you to perform operation, administration and maintenance (OAM) conveniently. On the Functions navigation tree, click “+” on the “EPON Management” node, and then double-click the extended leaf node “EPON OAM Management” to enter the [EPON OAM Management] dialog box shown in Figure 6-9. You can select different tabs to view different information.

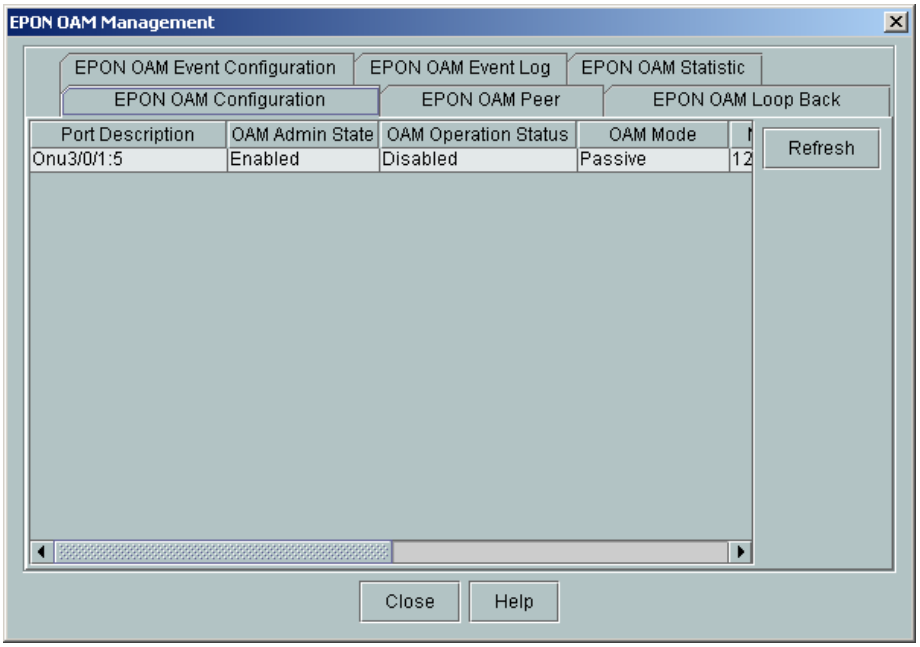


Figure 6-9 EPON OAM Management

6.6.1 EPON OAM Configuration

This function is used to view the OAM information of an ONU that is in UP state, including OAM administration state, OAM operation status, OAM mode, maximum OAM PDU size, OAM revision, supported OAM functions and so on.

6.6.2 EPON OAM Peer Information Browsing

This function is used to view the current state and configuration information of the OAM peer, including its status, MAC address, OUI, vendor information, mode, maximum size of OAM PDU, configuration revision, supported OAM peer functions and so on.

6.6.3 EPON OAM Loop Back

This function is used to control the loop back mode of ONU, including the OAM loop back command, OAM loop back status, and whether or not to process loop back command.

6.6.4 EPON OAM Event Configuration

This function is used to configure the thresholds of generating the standard Ethernet OAM events, including the error symbol period events, error frame period events, error frame events, and error frame summary events. This function also supports event notification which describes the link problems.

6.6.5 EPON OAM Event Log

This function is used to browse the latest 100 event logs, including such information as the timestamp of event, OUI of the entity OAM event type, event location, event window, event threshold, total number of running events, and total number of events.

Caution:

Only SNMPv2 supports the logging function.

6.6.6 EPON OAM Statistic

This function is used to browse the statistics of each ONU port, including the statistics about the transmitted and received OAM PDU, transmitted and received unique event OAM PDU, transmitted and received duplicate OAM PDU, transmitted and received loop back control OAM PDU, transmitted and received variable request OAM PDU, transmitted and received variable response OAM PDU, transmitted and received organization specific OAM PDU, transmitted and received unsupported op-code OAM PDU, and lost frames due to OAM.

6.7 EPON Device Management

On the Functions navigation tree, click “+” on the “EPON Management” node, and then double-click the extended leaf node “EPON Device Management” to enter the [EPON Device Management] dialog box shown in Figure 6-10.

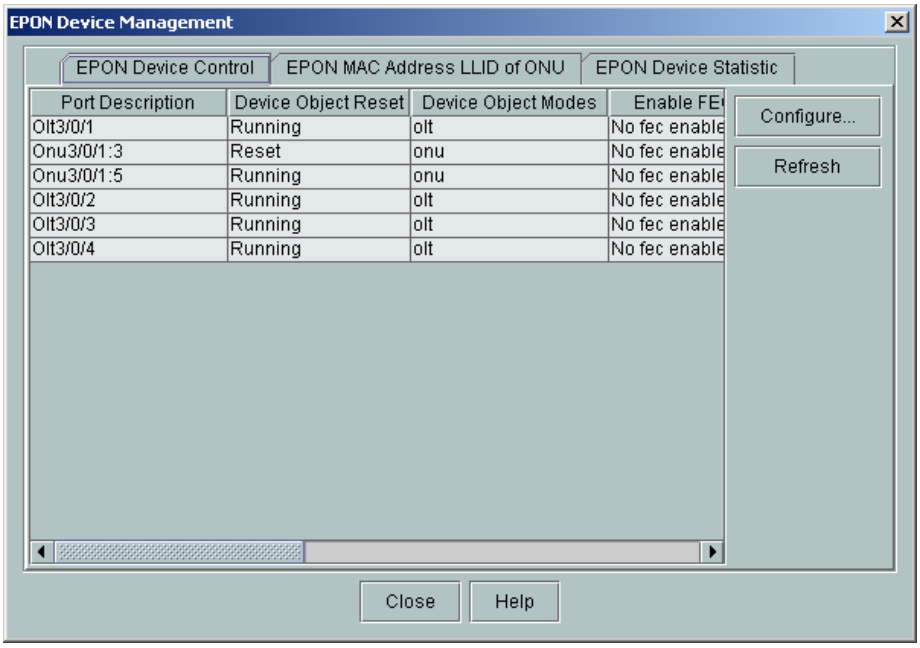


Figure 6-10 EPON Device Management

6.7.1 EPON Device Control

This function is used to enable the EPON device control function.

On the [EPON Device Management] dialog box, select the [EPON Device Control] tab to enter the [EPON Device Control] page. You can view such information as whether the device object is reset or running, device object modes, whether FEC is enabled, OAM mode, ready mode, whether the device is powered down, the number of LLID, report threshold, and the information about clearing EPON MAC-LLID address table of ONU.

Select the device to be reset, and click <Configure…> to open the [EPON Device Control] dialog box. Select the device object reset operation (Reset or Running), and click <OK>. You can make a reset OLT or ONU running by selecting **Running**, while you can make a running OLT or ONU reset by selecting **Reset**.

🕮 **Note:**

- Selecting **Running** does not take effect on a running OLT, and selecting **Reset** does not take effect on a reset OLT.
- The case for ONU is the same as that for OLT.

6.7.2 EPON MAC Address LLID of ONU

This function is used to view, add, configure, and delete related information of MAC address and LLID, including the name, LLID, ONU MAC address, MAC address type, and action on the LLID.

On the [EPON Device Management] dialog box, select the [EPON MAC Address LLID of ONU] tab to enter the [EPON MAC Address LLID of ONU] page to view related information. Click <Add…> to enter the [EPON MAC Address LLID of ONU] dialog box. Input a name, one of the queried remote MAC addresses, one of the queried LLID, and select one type of the queried MAC address types, and an action, and then click <OK>.

For the existing devices in the list, select one or more rows and click <Configure…> to enter the [EPON Device Event Configuration] dialog box. Select an action and click <OK>.

6.7.3 EPON Device Statistic

This function is used to display the times of transmitting, receiving and dropping frames of the queues on each OLT or ONU port.

6.8 EPON UNI Management

The UNI is an Ethernet interface on the ONU. EPON UNI management provides the following functions: UNI port management, UNI port traffic statistics, and display and management of UNI port multicast information.

In the function window, click "+" on the [EPON Management] node and double-click the extended leaf node [EPON UNI Management]. The system displays the [EPON UNI Management] dialog box, as shown in Figure 6-11.

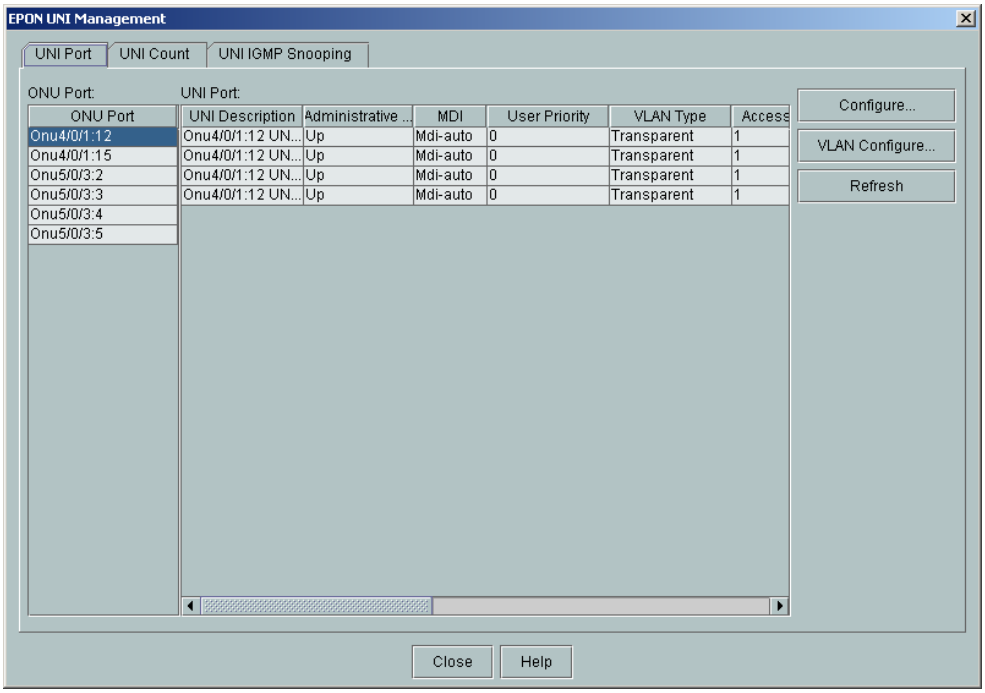


Figure 6-11 EPON UNI Management

6.8.1 UNI Port Management

This function is used to query and configure the UNI port parameters.

In the [EPON UNI Management] dialog box, select the [UNI Port Management] tab, and then select an ONU port in the ONU port list on the left. Then you can view the information of UNI ports under the selected ONU in the UNI port list on the right.

Select a record in the UNI port list and click <Configure…> to display the [UNI Port Configuration] dialog box, as shown in Figure 6-12. You can configure the related parameter in this dialog box.

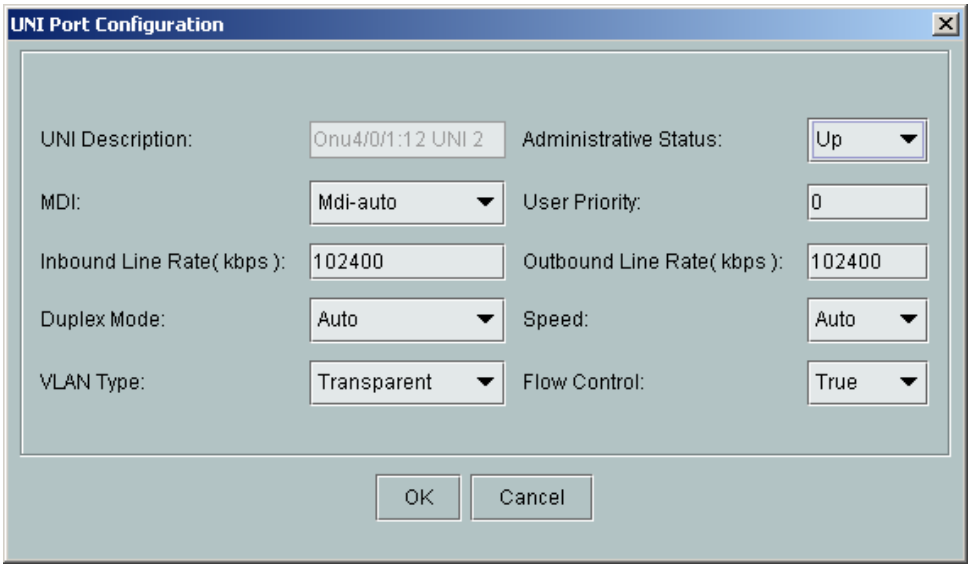


Figure 6-12 UNI Port Configuration

Table 6-11 lists parameters in the [UNI Port Configuration] dialog box and their means.

Table 6-11 Description of UNI port configuration parameters

Parameter	Description
Administrative Status	Administrative status of ONI port. Two options are available: Up and Down
MDI	Type of the network cable connecting the UNI port. Three options are available: Mdi-ii, Mdi-x, and Mdi-auto.
User Priority	The value ranges from 0 to 7. A larger value indicates a higher priority.
Inbound Line Rate (kbps)	Flow restriction on packets imported by the ONI port. The value range varies with the devices.
Outbound Line Rate (kbps)	Flow restriction on packets exported by the ONI port. The value range varies with the devices.
Duplex Mode	Working mode of the port. Three options are available: Full, Half, and Auto.
Speed	Speed of the UNI port. Three options are available: Auto, S10M, and S100M.
VLAN Type	Five options are available: Transparent, Trunk, Access, Hybrid and Untagged.
Flow Control	Enable or disable the flow control for the port. “True” means the flow control function is enabled and “False” disabled.

Select a record in the UNI port list on the right and click <VLAN Configure…>. You can configure the related parameter in the pop-up dialog box.

- If the VLAN type of the selected UNI port is “Trunk”, the [Trunk VLAN Configuration] dialog box is displayed. You can enter the VLAN ID and PVID that are allowed to pass the port according to the format requirement and then click <OK>.
- If the VLAN type of the selected UNI port is “Access”, the [Access VLAN Configuration] dialog box is displayed. You can enter the “Access VLAN” that is allowed to pass the port according to the format requirement and then click <OK>.

Note:

- UNI VLAN types supported by ET204 include Access, Trunk and QINQ. The UNI VLAN type is irrelevant to the ONU VLAN type and the ONU has its own VLAN types.
- You can only select one of the following options as the line rate of the ET204: 128, 256, 512, 1024, 2048, 4096, 8192, and 102400.
- During the configuration of Access VLAN, if the ONU configured is ET204, the “Access VLAN” configuration item is replaced by ““PVID”.

6.8.2 UNI Port Traffic Statistics

This function is used to query and monitor the traffic statistics information of UNI ports. The information includes Packets Received, Unicast Packets Received, Broadcast Packets Received, Multicast Packets Received, Pause Packets Received, Packets Received in Error, CRC Errors Received, Runts Received, Giants Received, Other Errors Received, Packets Sent, Unicast Packets Sent, Broadcast Packets Sent, Multicast Packets Sent, Pause Packets Sent, Packets Sent in Error, Collisions Sent, Deferred Errors Sent, and Other Errors Sent.

In the [EPON UNI Management] dialog box, select the [UNI Count] tab. Select an ONU port in the ONU port list on the left. Then you can view the traffic statistics information of the selected UNI port under the selected ONU in the UNI port list on the right.

Select a record in the UNI port list on the right and click <Clear> to clear the traffic statistics information of the selected UNI port.

Select a record in the UNI port list on the right and click <Monitor> to display the [Port Traffic Monitoring] dialog box, where the traffic statistics information of the selected UNI port is monitored.

6.8.3 UNI Port Multicast Information

This function is used to query the UNI port multicast information, including the UNI MAC address index and IGMP Snooping MAC address.

In the [EPON UNI Management] dialog box, select the [UNI IGMP Snooping] tab. Select an ONU port in the ONU port list on the right and you can view the multicast information of the UNIs under the selected ONU in the UNI port list on the right.

Chapter 7 VDSL Management

7.1 Overview

With the fast development of Internet market, the traditional low-speed services such as telephone, fax and telegraph cannot meet people's demands any more. Today the Internet services are expanding to broadband fields such as high-speed Internet access, video phone and video on demand (VoD). The access rate becomes the focus, therefore, the traditional audio dialing can no longer satisfy the increasing demands, and the age of broadband access has come.

VDSL (Very high speed Digital Subscriber Line) is one of the technologies providing broadband access. It can operate at symmetric and asymmetric rates, running with POTS (plain old telephone service) on the same twisted pair, mainly used in "the last kilometer" connection, transmitting voice, video and data to the multimedia network that provides overall services for users.

Essentially, VDSL technology is used to transport data over twisted pair cables, that is, with VDSL, voice service and data service are provided simultaneously over the subscriber line in frequency-division multiplexing mode and the signals of the two types are split by a splitter at the ends of the subscriber line.

The VDSL of the Quidview Device Manager is mainly used to manage S3026V remote Ethernet switch. Besides the functions (e.g. device information browsing and configuration, protocol configuration, VLAN configuration, port configuration and RMON) covered in the previous chapters, it provides VDSL management for the S3026V switch as well. The management function includes VDSL port configuration and port performance monitoring, which are detailed in the following sections.

7.2 VDSL Port Configuration

7.2.1 Browsing Port Link Data

Double-click on the [VDSL Management/Port Link Browse] node in the function pane to open the Information of [VDSL Port Link] dialog box, as shown in Figure 7-1.

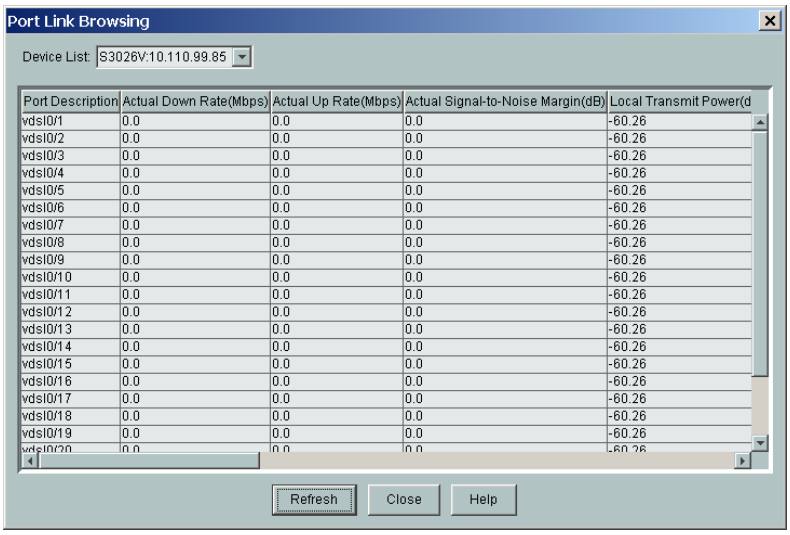


Figure 7-1 Information of VDSL port link

This interface is used to view the VDSL port link data, including the following parameters: Port Description, Actual Down Rate, Actual Up Rate, Actual Signal-to-Noise Margin, Local Transmit Power, Remote Transmit Power, Local Signal-To-Noise, Remote Signal-To-Noise, Local Mean Square Difference, Remote Mean Square Difference, Local RS Errors, Remote RS Errors, Downstream Channel Interleave Delay and Upstream Channel Interleave Delay.

7.2.2 Browsing Port Version Information

Double-click on [VDSL Management/Port Version Browse] node in the function pane to open the [Port Version Browsing] dialog box, as shown in Figure 7-2:

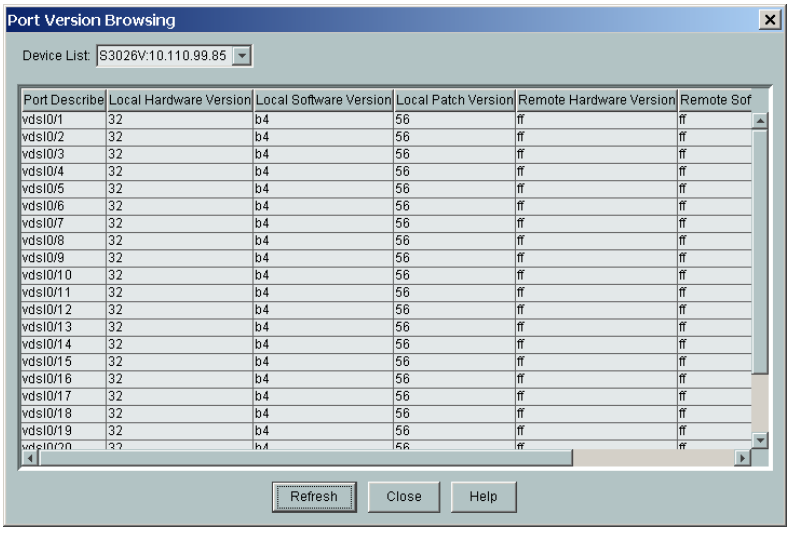

Port Version Browsing
Device List: S3026V:10.110.99.85
Port Describe
Local Hardware Version
Local Software Version
Local Patch Version
Remote Hardware Version
Remote Sof
vdsl0/1 32 b4 56 ff ff
vdsl0/2 32 b4 56 ff ff
vdsl0/3 32 b4 56 ff ff
vdsl0/4 32 b4 56 ff ff
vdsl0/5 32 b4 56 ff ff
vdsl0/6 32 b4 56 ff ff
vdsl0/7 32 b4 56 ff ff
vdsl0/8 32 b4 56 ff ff
vdsl0/9 32 b4 56 ff ff
vdsl0/10 32 b4 56 ff ff
vdsl0/11 32 b4 56 ff ff
vdsl0/12 32 b4 56 ff ff
vdsl0/13 32 b4 56 ff ff
vdsl0/14 32 b4 56 ff ff
vdsl0/15 32 b4 56 ff ff
vdsl0/16 32 b4 56 ff ff
vdsl0/17 32 b4 56 ff ff
vdsl0/18 32 b4 56 ff ff
vdsl0/19 32 b4 56 ff ff
Refresh
Close
Help

Figure 7-2 Port Version Browsing

This dialog box is used to browse the version information of all the VDSL ports, including the following parameters: Port Description, Local Hardware Version, Local Software Version, Local Patch Version, Remote Hardware Version, Remote Software Version, and Remote Patch Version.

7.2.3 Port Template Management

I. Browsing port template

Double-click on [VDSL Management/Port Template Management] node in the function pane to open the [Port Template Management] dialog box, as shown Figure 7-3:

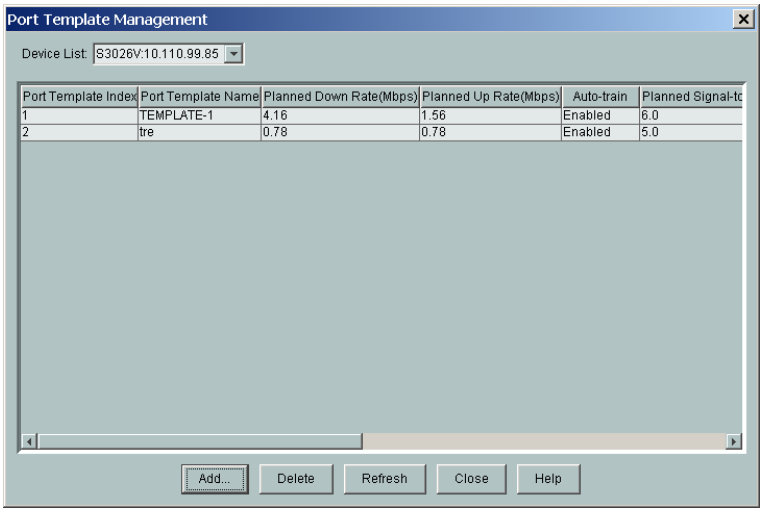


Figure 7-3 Port Template Management

The [Port Template Management] interface is used to browse the data of all port templates, including the following parameters: Port Template Index, Port Template Name, Planned Up/Down Row Rate, Enable Autotrain, Planned Signal-To-Noise, Enable Shield Amateur's Wireless Frequency Band.

II. Adding port template

Click <Add…> in the [Port Template Management] dialog box, and the [Create Port Template] dialog box appears, as shown in Figure 7-4. It is used to create a new port template.

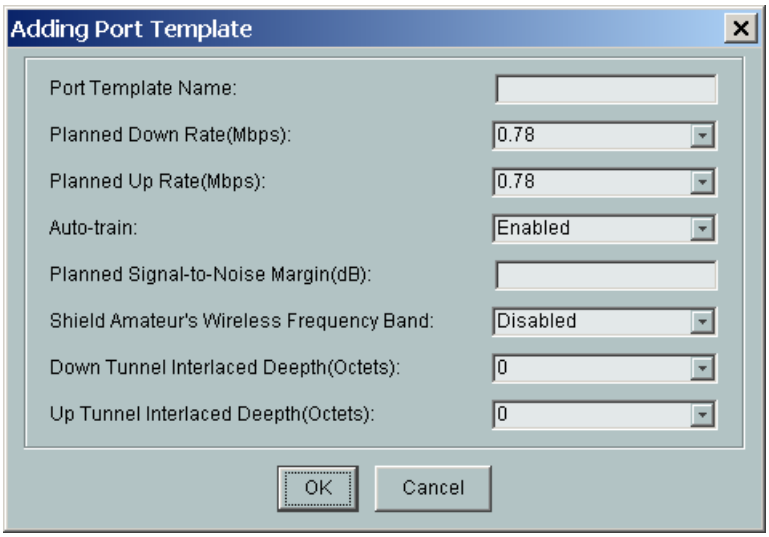


Figure 7-4 Adding Port Template

III. Deleting port template

In the [Port Template Management] interface, select one or multiple rows, and click <Delete>. The specified port template will then be deleted.

7.2.4 Port Parameter Configuration

I. Browsing VDSL port parameters

Select the [VDSL Management/Port Parameters Management] node from the function pane to open the [Port Parameter Management] dialog box, as shown in Figure 7-5:

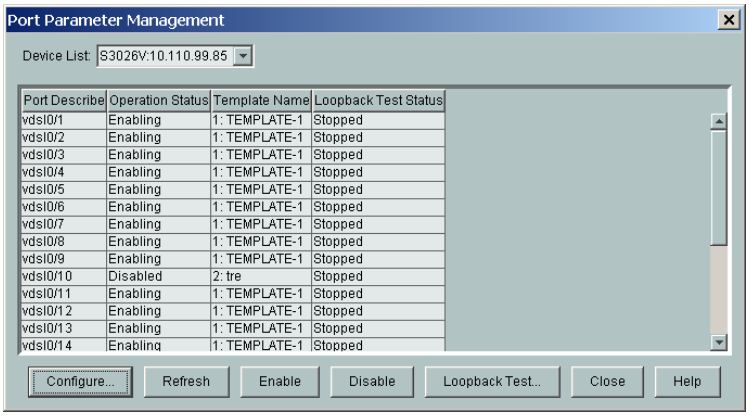

Port Parameter Management
Device List: S3026V:10.110.99.85
Port Describe | Operation Status | Template Name | Loopback Test Status
vdsl0/1 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/2 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/3 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/4 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/5 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/6 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/7 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/8 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/9 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/10 | Disabled | 2: tre | Stopped
vdsl0/11 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/12 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/13 | Enabling | 1: TEMPLATE-1 | Stopped
vdsl0/14 | Enabling | 1: TEMPLATE-1 | Stopped
Configure...
Refresh
Enable
Disable
Loopback Test...
Close
Help

Figure 7-5 Port Parameter Management

This dialog box is used to browse the parameter information of all VDSL ports, including Port Description, Administration Status, Template Name and Test Status.

II. Configuring VDSL port parameter

Select any row of data in the [VDSL Port Parameters Management] interface, click <Configure…>, then the [Configure Port Template] dialog box appears, as shown in Figure 7-6.

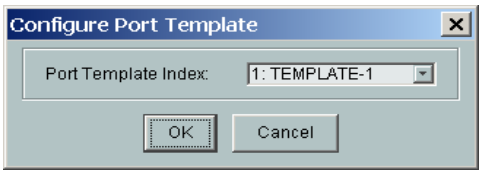


Figure 7-6 Configuring Port Template

Note:

You can only modify the templates of the inactivated ports.

III. Activating a VDSL port

Select one or more ports with the status as “Deactivate” from the [VDSL Port Parameters Management] interface and click <Active> to change the status to “Activate” or “Activating”.

IV. Deactivating a VDSL port

Select a VDSL port which is in “Activate” or “Activating” status from the [VDSL Port Parameters Management] interface. Click <Deactive> to change the port's status to “Deactivate”.

V. Loopback test

Select one or more VDSL ports from the [VDSL Port Parameters Management] interface, and click <Loopback>. The [Loopback Test] interface, where you can configure the loopback test type, as shown in Figure 7-7:

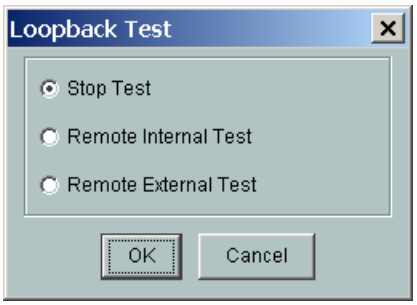


Figure 7-7 Port Loopback Test

7.3 VDSL Port Performance Monitoring

The main function of VDSL port performance monitoring is to monitor the performance of a VDSL port according to the selected monitoring mode and monitoring items. The operation is introduced as follows:

Select a port in the device panel view and double-click on [VDSL Management/Port Performance Management] node in the function pane to open the [VDSL Port Performance Monitor] interface, as shown in Figure 7-8.

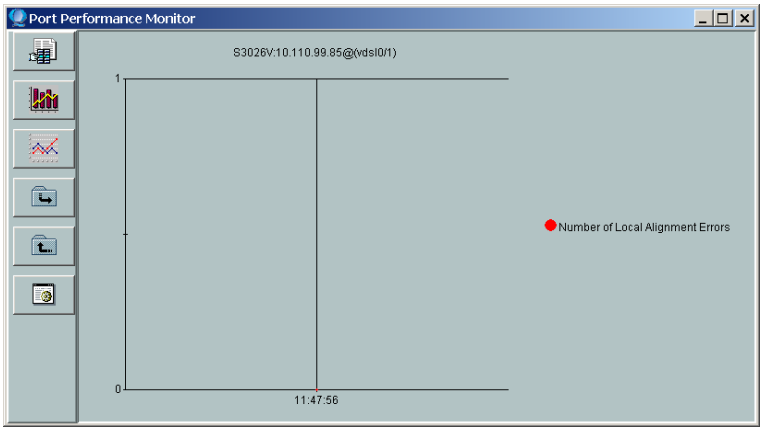


Figure 7-8 VDSL Port Performance Monitor

Chapter 8 Cluster Management

8.1 Overview

The cluster of Quidview Device Manager is divided into two types, V1 cluster and V2 cluster, where V1 cluster uses the HGMP V1 and V2 cluster uses the HGMP V2.

8.1.1 Concept of Cluster

I. Concept of V1 cluster

The HGMP V1 is a communication protocol that implements concentrated management and L2 multicast group control by management processes (e.g. multi-service access concentrator of high-end device) over agent processes (e.g. L2 switch connected to multi-service access concentrator downstream). Its basic structure is a management process managing several agent processes simultaneously. The HGMP running in management and agent processes is called HGMP server switch (SERVER) and HGMP client switch (CLIENT) respectively, which constitute the HGMP V1 cluster management. The typical application environment of HGMP V1 cluster is illustrated in the following figure:

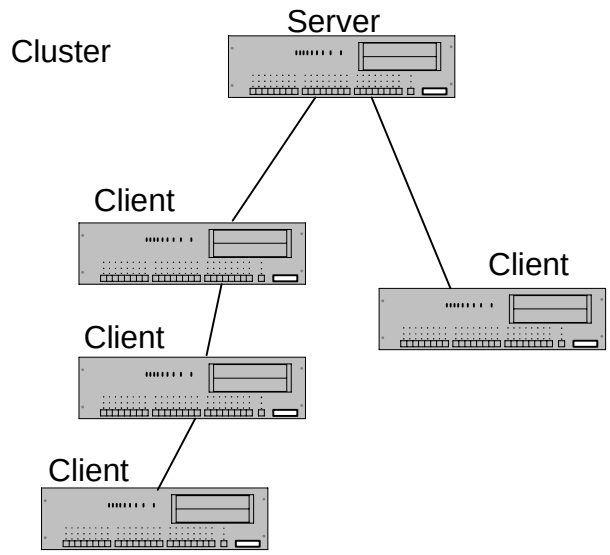


Figure 8-1 HGMP V1 cluster

Depending on the locations and functions, the switches in a cluster can play the following roles:

1) Server switch

It is the switch assigned with a public network IP address, which provides the management interfaces for the overall cluster. A management command is first sent to the server switch for being processed. If it finds that the command is destined to a certain client switch, it will redirect the command to the client switch.

2) Client switch

It is a client of a cluster, which is not assigned with a public network IP address in normal situations. It only receives the management commands redirected from the server switch.

II. Concept of V2 cluster

V2 cluster is a manageable network comprising of multiple interconnected switches, which is assigned with a single IP address. All switches in the cluster must support HGMP V2. With cluster management, the user can manage a group of switches without assigning an IP address to each member switch.

Depending on the locations and functions, the switches in a cluster can play the following roles:

1) Command switch

It is the switch assigned with a public network IP address, which provides the main management interfaces for the overall cluster. A management command is first sent to the command switch for processing. If it finds that the command is destined to a certain member switch, it will redirect the command to the member switch.

2) Member switch

It is a member of a cluster, which is not assigned with a public network IP address in normal situations. It only receives the management commands redirected from the command switch.

3) Candidate switch

Candidate switch refers to the switch that does not join any cluster, but has the cluster capability and can become a member of a cluster.

4) Independent switch

Independent switch refers to the switch that can be discovered in the process of gathering cluster topology information, but has no cluster capability and cannot become a cluster member.

The process of establishing a cluster and the role changing rules for the switches are shown in Figure 8-2.

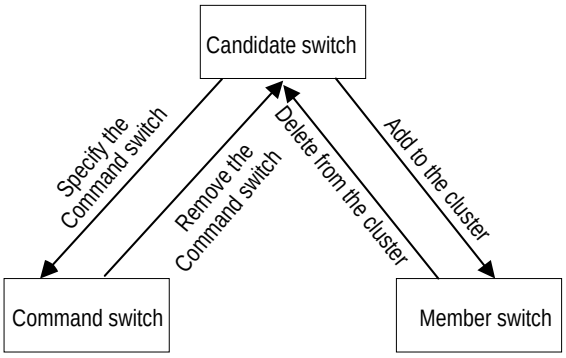


Figure 8-2 Process of establishing cluster and role changing rules for switches

First, the network administrator manually specifies a switch to be the command switch via the network management port or CLI (Command Line Interface). Then, the command switch gathers the device topology information for discovering and determining the candidate switches. The user can make a candidate switch a cluster member by adding it to a cluster through configuration. After a member switch is removed from the cluster, it will become a candidate switch again.

8.1.2 Features of Cluster

The main purpose of cluster management is to enable network administrators to manage multiple switches through the single public network IP address of a command switch. To sum up, cluster has the following features:

- Rather than making initial configurations on the console of each member (client) switch, the user only needs to assign an IP address to the command (server) switch for managing and configuring multiple switches. It greatly simplifies the configuration management tasks.
- Provides the topology discovery and displaying functions, which facilitate network monitoring and debugging.
- Manages multiple switches with a single IP address, which saves the precious IP address resources.
- Concurrently upgrades software and sets parameters on multiple switches, which streamlines the device management.
- Independent of topology and distance, cluster can be used conveniently.

8.1.3 Cluster Management of Quidview Device Manager

I. V1 Cluster Management

As a feature of Quidview Device Manager, V1 cluster management primarily provides the following functions:

1) Cluster management and maintenance, including:

- Creating and deleting cluster, and displaying the role and status of each switch and the connections among various switches on topology views in the format of different icons.
- Refreshing cluster, reading latest cluster topology information and updating topology views.
- Configuring server switch port parameters, and browsing and configuring port HGMP V1 status (supporting managing several ports on a device simultaneously).

2) Configuration and management of server switch and client switches, including:

- Opening server switch panel to conduct protocol/service (such as VLAN and QoS) configuration and browsing.
- Opening client switch management window to configure single or batch VLANs, ports and link aggregations.
- Batch accessing, saving, erasing client switches' configurations.
- Batch upgrading client switches' mapping/bootrom files.
- Batch rebooting client switches.

3) Other functions:

- View management: includes displaying/hiding the labels of the switches, saving view, automatic layout, and displaying the overview.
- Link traffic: displays the traffic of the link between the start and end ports in the format of a fold-line graph.

II. V2 Cluster Management

The V2 cluster management of Quidview Device Manager contains the following three aspects:

- Management and maintenance of cluster

The cluster management and maintenance includes establishing a cluster, opening a cluster, closing a cluster, adding member switches to a cluster and delete them from the cluster, deleting a cluster, etc.

- Device management and configuration

The user can manage and configure the Ethernet switches, including the command switch and member switches, in a cluster, in the corresponding device panel views after opening them.

- Auxiliary functions

Auxiliary functions mainly include link traffic display, topology information saving, setting saving, candidate switches displaying and setting parameters. Link traffic display can be used to dynamically show the traffic information on the link selected by the user in the report format or in the form of grid and graph. Topology saving enables the user to change the device layout in the topology graph of his choice, and save the changed topology graph. The function of saving settings is used to write the configurations that the user makes on the switches onto the switches at a time. Candidate switches display function can be used to set whether the graph of candidate

switches will be displayed when opening the cluster topology graph. The function of parameter setting is used to set some cluster-related parameters in common use.

8.2 V1 Cluster Management

8.2.1 Cluster Creation and Maintenance

I. New cluster

After Quidview Device Manager starts, open the device serves as the cluster Server switch, click the "+" on the "Cluster Management" node in the function navigation pane and then double-click the unfolded "New V1 Cluster" node; the system pops up the [New V1 Cluster] dialog box, as shown in Figure 8-3.

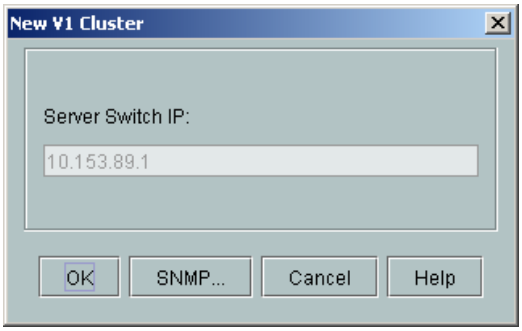


Figure 8-3 New V1 cluster

Click <SNMP…> to configure the SNMP parameters, and then click <OK> to create a new V1 cluster. If the creation succeeds, its topology view will be opened.

The other creation mode is to select a certain Server switch from the opened V2 cluster topology, and then select "Create V1 Cluster" in the right-click popup menu. If it is successfully created, the topology view of V1 cluster is opened.

II. Opening cluster

There are four kinds of modes to open an existing V1 cluster: Select [Device/Open Device…], input the IP address of the Server switch in the popup [Open Device] dialog box, and click <OK>; click on the toolbar, input the IP address of the Server switch in the popup [Open Device] dialog box, and click <OK>; select the Server switch on the Device List navigation window, and select "Open Devices…" in the pop-up menu; select a certain Server switch on the opened V2 cluster topology, select "Open V1 Cluster" in the pop-up menu. After it is successfully created, the system shows the topology of V1 cluster.

III. Deleting cluster

Select the Server switch in the V1 cluster topology, and select [Delete Cluster] in the pop-up menu or directly double-click on [Cluster Management/Delete Cluster] node in

the function pane. The system shows “Are you sure to delete it” dialog box, and you can click <OK> to delete the cluster and its members from the system. If the V1 cluster is created or opened from V2 cluster, it returns to the topology of V2 cluster after it is closed.

IV. Returning to senior cluster

If the V1 cluster is created or opened from V2 cluster, the user can right-click the blank in the V1 topology, select “Return Senior Cluster” in the pop-up menu, or directly double-click [Cluster Management/Return Senior Cluster] in the function pane to close V1 cluster and return to V2 cluster topology.

V. Saving configuration

In the V1 cluster topology, select [Save Configuration] in the pop-up menu or double-click [Cluster Management/Save Configuration] in the function pane. The system pops up the prompt dialog box. Click <OK>, and the system saves the cluster information in Server switch.

VI. Opening panel

In the V1 cluster topology, select [Open Panel] in the pop-up menu of the server switch or directly double-click on [Cluster Management/Open Panel] in the function pane. The system pops up the panel of the Server switch and performs device configuration management.

VII. Setting parameter

In the V1 cluster topology, select [Set Parameter] in the pop-up menu of topology or directly double-click [Cluster Management/Set Parameter] in the function pane. The system pops up the dialog box that allows you to set HGMP V1 protocol parameters for each port of Server switch.

8.2.2 Client Switch Management

Select one or multiple Client switches in the V1 cluster topology, double-click [Client Management/Client Management] in the function pane, or select [Client Management] in the pop-up menu. Thus, the system opens the configuration interface of the selected Client switch as shown in Figure 8-4. Through the interface, the user can manage and configure the selected Client switch, including parameter configuration, VLAN configuration management, port aggregation management, port mirroring management, and port management.

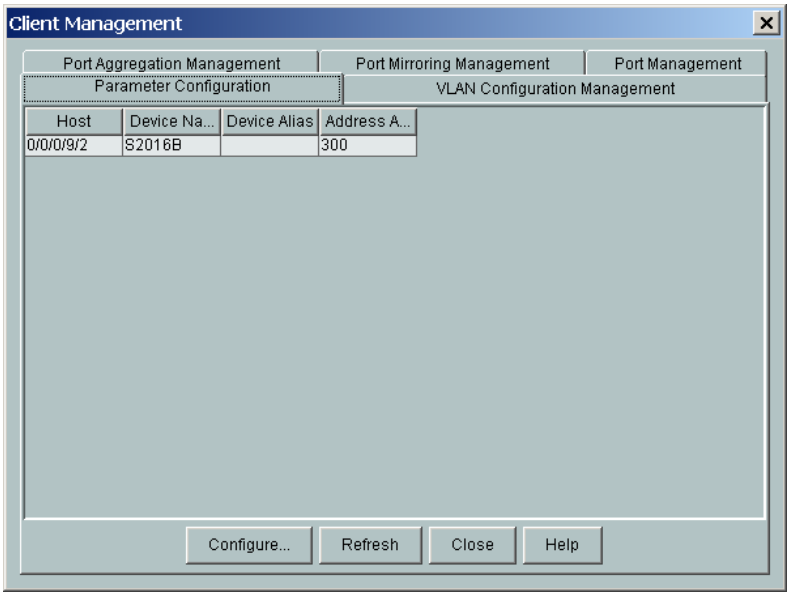


Figure 8-4 Client management

I. Basic information configuration

Select the [Parameter Configuration] tab in Figure 8-4, and then select a line of data (one line represent one client switch). Click <Configure…>, and the [Parameters Configure] dialog box pops up. Thus, the following parameters can be configured: device name, address aging time, and device alias, etc.

The address aging time is in second, and the range is 0 to 1048575. The switch will learn the MAC address of the connected host. In the ranged aging time, if it hasn't received the registration information of the corresponding host, it assumes that the MAC address is invalid and learns the address again.

II. VLAN management

Select the [VLAN Configuration Management] tab in Figure 8-4, and enter the configuration management interface shown in Figure 8-5. Click <Configure…>, the dialog box shown in Figure 8-6 pops up, and VLAN data can be modified. Click <Add…>, and the dialog box shown in Figure 8-7 pops up, which allows you to add a new VLAN. Click <Refresh>, all the latest VLAN information of the host is displayed.

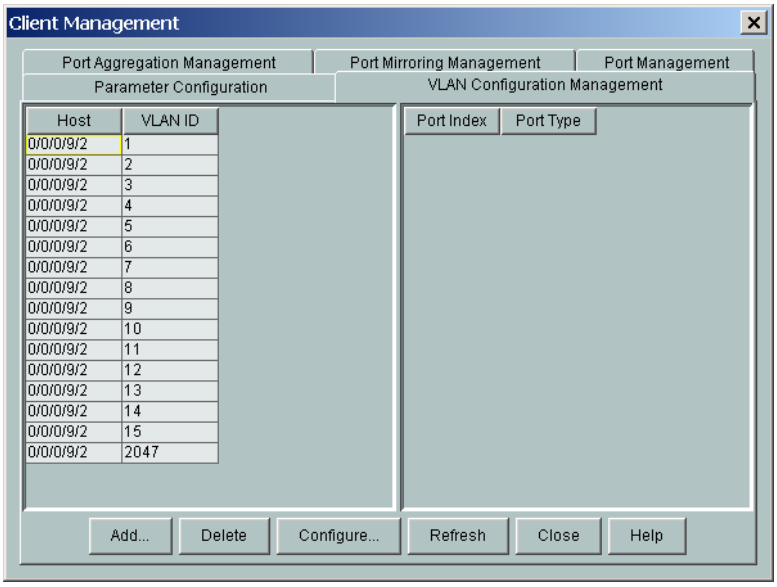


Figure 8-5 VLAN configuration management

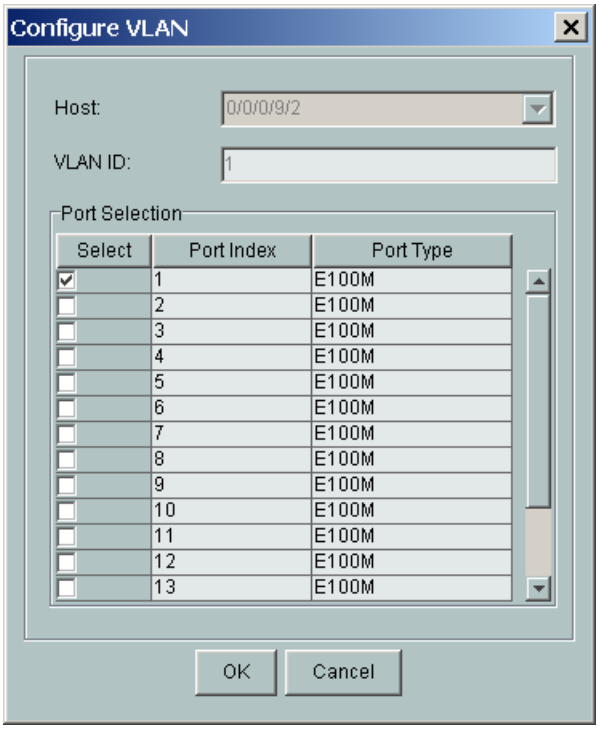


Figure 8-6 VLAN configuration

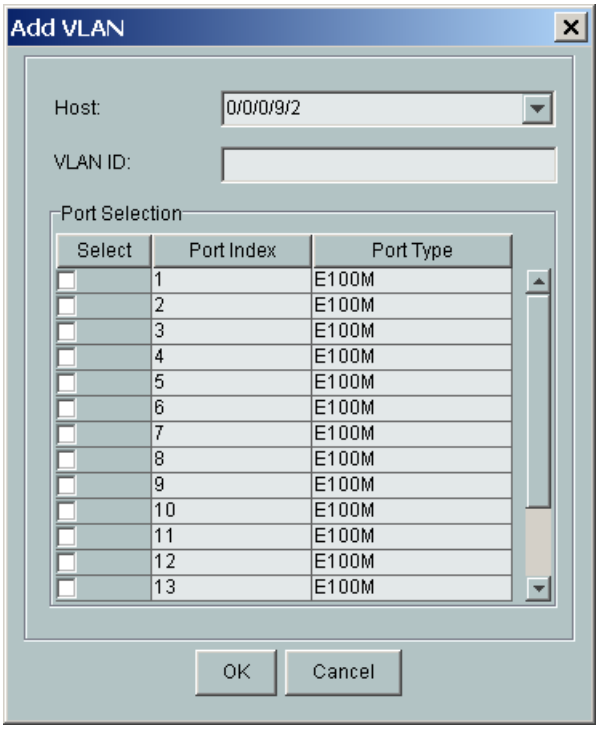


Figure 8-7 Adding a VLAN

III. Port aggregation management

Select the [Port Aggregation Management] tab in Figure 8-4, and enter the port aggregation management interface. Click <Configure…>, and the corresponding dialog box appears. Thus, you can modify the port aggregation data. Click <Refresh>, and all the latest port aggregation information of the host is displayed.

IV. Port mirroring management

Select the [Port Mirroring Management] tab in Figure 8-4, and enter the port mirroring management interface shown in Figure 8-8. Click <Configure…>, the dialog box shown in Figure 8-9 pops up, and the port mirroring data can be modified. Click <Refresh>, and all the latest port mirroring information of the host is displayed.

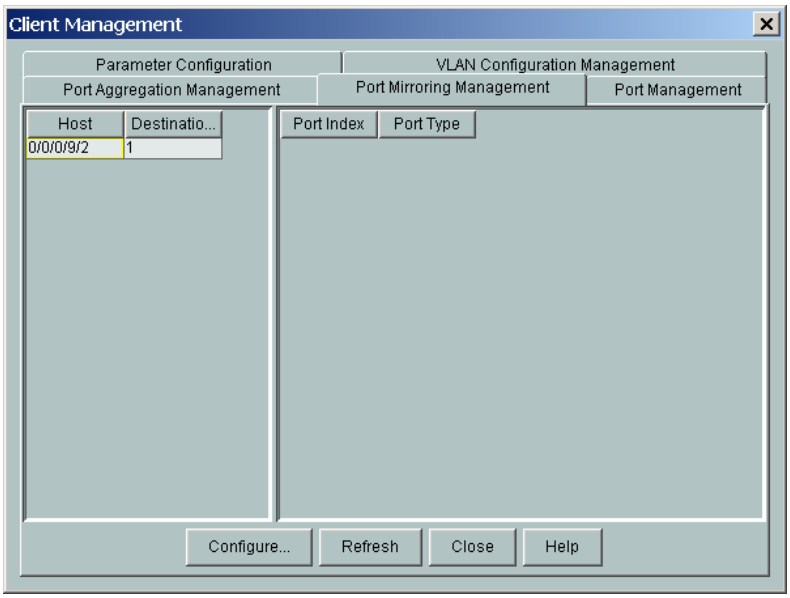


Figure 8-8 Port mirroring management

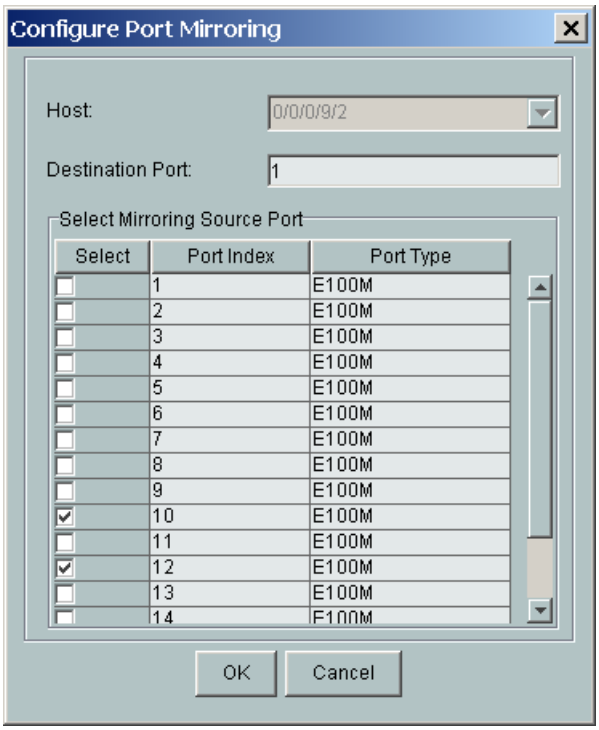


Figure 8-9 Configuring port mirroring

V. Port management

Select the [Port Management] in Figure 8-4, and enter the port configuration management interface shown in Figure 8-10. Click <Configure…>, the dialog box

shown in Figure 8-11 pops up, and the port data can be modified. Click <Refresh>, and all the latest port information of the host is displayed.

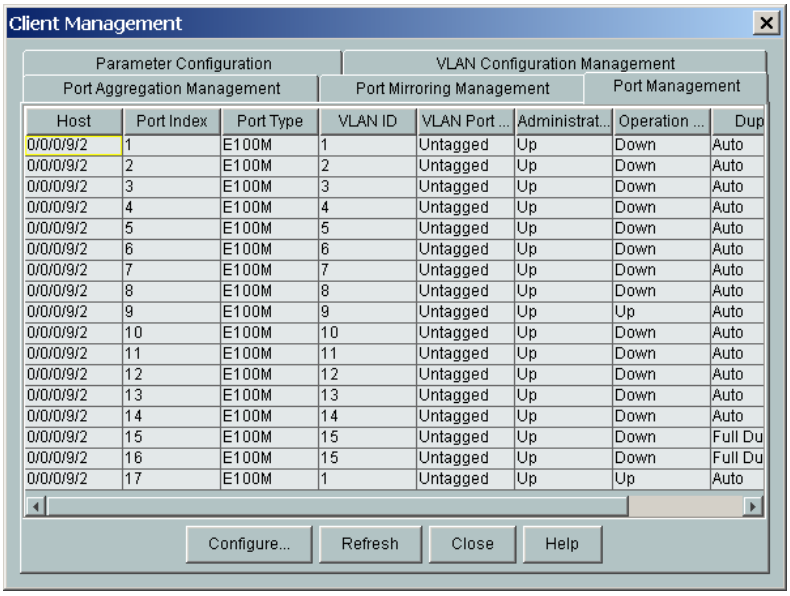

Client Management
Parameter Configuration
VLAN Configuration Management
Port Aggregation Management
Port Mirroring Management
Port Management
Host
Port Index
Port Type
VLAN ID
VLAN Port ...
Administrat...
Operation ...
Dup
0/0/0/9/2 1 E100M 1 Untagged Up Down Auto
0/0/0/9/2 2 E100M 2 Untagged Up Down Auto
0/0/0/9/2 3 E100M 3 Untagged Up Down Auto
0/0/0/9/2 4 E100M 4 Untagged Up Down Auto
0/0/0/9/2 5 E100M 5 Untagged Up Down Auto
0/0/0/9/2 6 E100M 6 Untagged Up Down Auto
0/0/0/9/2 7 E100M 7 Untagged Up Down Auto
0/0/0/9/2 8 E100M 8 Untagged Up Down Auto
0/0/0/9/2 9 E100M 9 Untagged Up Up Auto
0/0/0/9/2 10 E100M 10 Untagged Up Down Auto
0/0/0/9/2 11 E100M 11 Untagged Up Down Auto
0/0/0/9/2 12 E100M 12 Untagged Up Down Auto
0/0/0/9/2 13 E100M 13 Untagged Up Down Auto
0/0/0/9/2 14 E100M 14 Untagged Up Down Auto
0/0/0/9/2 15 E100M 15 Untagged Up Down Full Du
0/0/0/9/2 16 E100M 15 Untagged Up Down Full Du
0/0/0/9/2 17 E100M 1 Untagged Up Up Auto
Configure...
Refresh
Close
Help

Figure 8-10 Port management

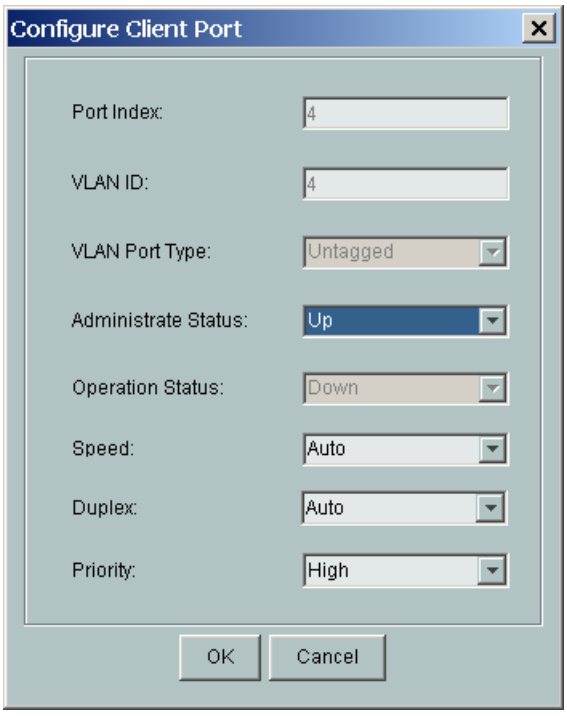


Figure 8-11 Configuring client port

VI. Restarting device

Right click on one or more client switches, and select [Restart Device] from the pop-up menu, or double-click [Client Management/Restart Device] in the function pane. The

system pops up the prompt dialog box to ask you whether to restart the device. Click <OK> to restart the device.

VII. Updating software

Select one or multiple Client switches, and select “Update Software” in the pop-up menu, or double-click [Client Management/Update Software] in the function pane. The system pops up the “software updating management” dialog box. Select the type of software update: bootrom file or app file. Click <OK> after inputting the file name. Update the client switch with the corresponding update file on the Server switch.

VIII. Obtaining configuration

Select one or more Client switches, and select [Get Configuration to Server] in the pop-up menu, or double-click [Client Management/Get Configuration to Server] in the function pane. The system pops up the prompt dialog box to ask you whether to operate. Click <OK> and the configuration of the client switch is saved to the server switch. In this way, the configuration file can be obtained from the server when the client is restarted next time.

⚠ **Caution:**

When Client is started, whether to use the software saved in Server switch is determined by the type of device. Refer to the user manual of specific devices.

IX. Saving configuration

Select one or multiple Client switches, and select “Save Configuration” in the pop-up menu, or double-click [Client Management/Save Configuration] in the function pane. The system pops up the prompt dialog box to ask you whether to operate. Click <OK> and the configuration of the client switch is saved to its Flash.

X. Erasing configuration

Select one or multiple Client switches, and select [Erase Configuration] in the pop-up menu, or double-click [Client Management/Erase Configuration] in the function pane. The system pops up the prompt dialog box to ask you whether to operate. Click <OK> to erase the Flash configuration of the client switch.

8.2.3 Other Functions

I. Link traffic

Select one connection between Server switch and Client switch or between Client switch and Client switch in the cluster topology, and double-click [Performance Monitoring/Link Traffic] in the function pane or select [Link Traffic] in the pop-up menu. The system shows the traffic diagram of the connection.

II. Showing/Hiding label

Right-click the blank of the cluster topology, and select [Show/Hide Label] in the pop-up menu, or double-click [View Management-Show/Hide Label] in the function pane. Thus, the label of the switch can be shown or hidden. If the node representing the switch in the previous topology is unlabeled, it will be labeled now; otherwise, it will change from labeled to unlabeled.

III. Saving view

The user can adjust the device location in the topology as required and save the adjusted topology. When the cluster is opened next time, it shows the topology view saved by the user. The other advantage is that when there are multiple devices, it may increase the speed to open the device and prompt the user to see the network topology immediately. Then, the system refreshes it at daemon.

Right-click the blank in the topology of the cluster, select [Save Map] in the pop-up menu, or double-click [View Management/Save Map] in the function pane, and save the topology view in the format of “MAC address”.ilv and “MAC address”.top.

8.3 V2 Cluster Management

8.3.1 Cluster Creation and Maintenance

I. New cluster

Start Quidview Device Manager, open the device serves as the V2 cluster command switch, click the “+” on the “Cluster Management” node in the function navigation pane and then double-click the unfolded “New Cluster” node; the system pops up the [New Cluster] dialog box, as shown in Figure 8-12.

Figure 8-12 New Cluster Information

Input the corresponding parameters in the dialog box, click <Auth…> to configure the authentication parameters, and then click <OK> to create a new cluster. For the parameter meaning, refer to Table 8-1.

Table 8-1 Description of parameters in the [New Cluster] dialog box

Parameter	Description
Command Switch IP	Public network IP address of the command switch.
Cluster Name	Specifies a name for the new cluster.
Private Network Start IP	Assigns private start IP addresses for the member switches in the cluster. Along with the next argument “private network mask”, it determines the private segment for the member switches in the cluster.
Private Network Mask	Subnet masks of the private IP addresses used by the member switches in the cluster.

II. Opening cluster

Start Quidview Device Manager, select the menu option [Device/Open Device…] or click the button on the toolbar. In the popup [Open Device] dialog box, input the IP address of the command switch in a cluster and correct authentication parameters. Then, click <OK> to open an existing V2 cluster. The system will display the topology map of the cluster.

III. Adding a member switch

Select a candidate switch in the cluster topology map, and double-click on [Cluster Management/Add Member] node in the function pane or select [Add Member] from the pop-up menu. In the popup dialog box, input the MAC address and super password of

the switch to add the candidate switch to the cluster. Thus, the candidate switch becomes a member switch of the cluster.

🕮 **Note:**

If you select a candidate switch in the V2 topology map and then add it to a cluster, you do not need to input the MAC address of the switch.

IV. Deleting a member switch from a cluster

Select a member switch in the V2 cluster topology map, and double-click on [Cluster Management/Delete Member] node in the function pane (or select [Delete Member] from the pop-up menu) to delete the member switch from the cluster. Thus, the member switch becomes a candidate switch again.

V. Deleting a Cluster

Select the command switch in the V2 cluster topology map, and select [Delete Cluster] from the pop-up menu (or directly select [Cluster Management/Delete Cluster] node from the function pane). Click <OK> in the popup confirmation dialog box and delete the cluster along with its all members from the system.

VI. Opening panel

Select one or more switches from the V2 cluster topology map, double-click on [Cluster Management/Open Panel] node or select [Open Panel] from the pop-up menu to open the device panel view of the switch. In the panel view, the user can manage and configure the switch, such as browsing and configuring device information, configuring ports, configuring VLAN and protocols, etc.

VII. Setting parameters

Select [Cluster Management/Set Parameters] node from the function pane to set the parameters for a cluster, as shown in Figure 8-13.

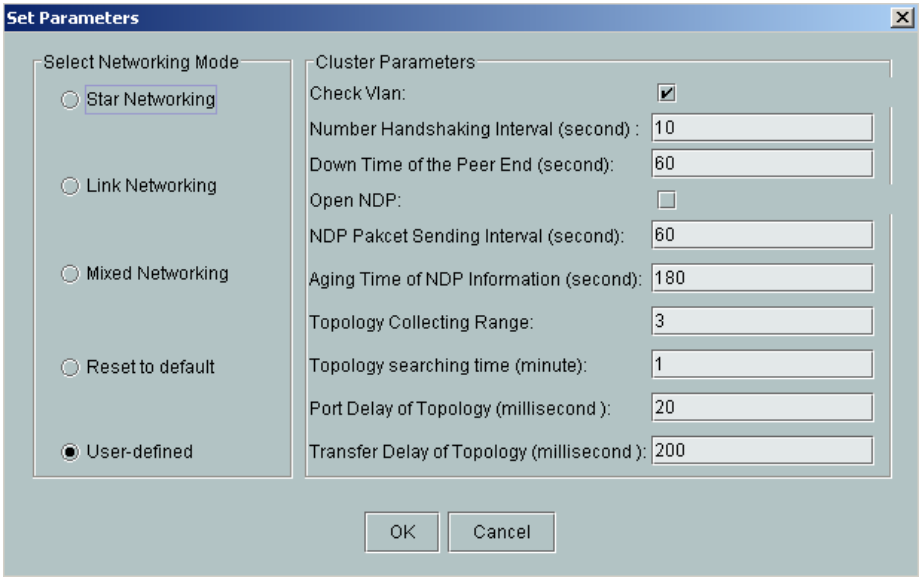


Figure 8-13 Setting cluster parameter information

Setting cluster parameters comprises two steps, selecting networking mode and setting cluster parameters, which will be covered below in details.

1) Selecting networking mode

Four networking mode options are available: “Star Networking”, “Link Networking”, “Mixed Networking” and “User-defined”. The parameters for the first three options are fixed, so the user cannot make configurations. In normal circumstances, the user is expected to choose the “User-defined” option.

2) Cluster parameters

- Check VLAN: This parameter is configured to determine whether VLAN security check will be implemented on the communications within a cluster.
- Member handshaking Interval: Within a cluster, real-time communications between the member switches and the command switch are maintained through sending the handshaking packets. After a switch is placed in a cluster, it begins to regularly shake hands with the command switch by sending handshaking packets.
- Down Time of the Peer End: After a cluster is created, communication failures may occur due to the network faults or switch reboot. If the failure duration of a member exceeds the specified valid retaining interval, its state will be shown as “down”. After the communication recovers, the corresponding member device will be added to the cluster again (the process is automatic). If the failure duration does not exceed the specified valid retaining interval, the member device remains in normal state and does not need to be added to the cluster again.
- Open NDP: NDP is used to discover information of the directly connected neighbor, including type of the adjacent device, software/hardware version, connection port, as well as device ID, port address, device capacity, and hardware platform. After NDP is opened, NDP information will be gathered regularly for user inquiry. If it is

disabled, all NDP information reserved in the switch will be cleaned up, and the switch will not process any NDP packets.

- NDP Packet Sending Interval: NDP information of the adjacent nodes should be refreshed in real time so as to ensure that the local device can know the latest changes made to the adjacent node information in time. Interval of transmitting NDP packets determines the frequency of refreshing NDP information.
- Aging Time of NDP Information: This parameter determines the valid time for NDP information to be held on the adjacent nodes. After the aging time, NDP information will be discarded. Normally, the hold-time of NDP information in neighbors should be greater than the NDP transmitting interval. Otherwise, it may cause instability of NDP information table.
- Topology Collecting Range: Specifies the range of devices, from which the topology information will be gathered. Thereby, gathering process can be prevented from infinitely spreading. For example, if the gathering range is set to 2, only the topology of the switches, which is two hops next to the switch generating the topology gathering request, will be gathered.
- Topology Searching Time: To learn the changes in the topology map in time, the command switch needs to regularly trigger topology collection of all devices in the specified range. The partial collection cannot reflect all changes in the topology map. By default, it is 0. That is, the command does not trigger topology collection actively.
- Port Delay of Topology: Network congestion or topology gathering device unavailability may occur, if a great number of network devices concurrently send topology response packets. In case of that, each port of the devices required for providing topology will wait for a certain period of time after receiving the request. After that period of time, the next port begins to forward the topology-gathering packet.
- Transfer Delay of Topology: Network congestion or topology gathering device unavailability may occur, if a great number of network devices concurrently send topology response packets. In this case, each device required for providing topology will wait for a certain period of time after receiving the request. After that period, the first port begins to forward the topology-gathering packet.

VIII. Creating V1 cluster

Select the member switch in the V2 cluster topology map, and then double-click [Cluster Management/Create Cluster V1] in the function navigation window, or right-click on the member switch and select [Create Cluster V1] from the pop-up menu. The system sets the switch as the server switch of V1 cluster and opens its topology.

IX. Opening V1 cluster

Select the member switch in the V2 cluster topology map, and then double-click [Cluster Management/Open V1 Cluster] in the function pane, or right-click on the

member switch and select [Open V1 Cluster] from the pop-up menu. The system opens the topology with the switch as the V1 cluster (regarding the switch as the server switch).

X. Saving settings

Save Configuration is used to save the modifications that the user has done to the device configuration files. Double-click [Cluster Management/Save Configuration] node in the function pane, and the system will write the current switch settings of the command switch and member switches into the corresponding devices. Notice that this process may take a relatively long time, if there are many switches in the cluster.

8.3.2 Other Functions

I. Link traffic

Select whichever link between switches, command-to-member or member-to-member, in the cluster topology map, and select [Performance Monitor/Link Traffic] node from the function pane (or right click on the link and select [Link Traffic] item from the pop-up menu) to display the link traffic diagram.

II. Displaying/Hiding switch

Display/Hide Switch is used to display/hide candidate or independent switches in current cluster topology. In the function pane, double-click on [Map Management/Show/Hide Candidate Switch] node to display or hide candidate switches; double-click [Map Management/Show/Hide Independent Switch] node to display or hide independent switches.

III. Displaying/Hiding label

Display/Hide Label is used to switch the labels of the switches in the interface. To enable this function, double-click [Map Management/Show/Hide Label] node in the function pane. After switchover, the device type and device name of each command or member switch will be displayed in the format of "device type: device name". For the candidate and independent switches, the MAC address will be displayed.

IV. Saving map

Save Map is used to save the current topology map of the cluster. Double-click [Map Management/Save Map] in the function navigation window, and the system saves the topology map of the cluster and shows the same topology map when it is opened next time.

V. Automatic layout

It is used to display the cluster topology map in different modes. By default, tree-structured view is displayed.

VI. Overview

It is used to form a panorama of a cluster's main view. When a view is large, you can select different area from the panorama to browse corresponding part of the cluster.

Chapter 9 Stack Management

9.1 Overview

9.1.1 Concept and Features of Stack

The stack is a management domain composed of a group of switches, including a command switch and several member switches. The stack uses a public IP address to implement management over all switches in it.

The creation procedure of a stack is as follows: Firstly, connect several switches to the stack ports of the stack module. Then perform either of the following operations:

- Create a stack directly under the NMS.
- Specify the public IP address of the command switch manually via the CLI and enable the stack function. Then the command switch will search for the switches connected to its stack port, add them to the stack as member switches, and configure their IP addresses automatically. Thus a stack is created.

With its basic characteristics mentioned above, the stack technology makes it possible to manage a large amount of low-end devices simultaneously, and to provide a unified network management interface for users. This facilitates the management and maintenance over many devices. The command switch is available with a management interface for stack management. When a member switch is added to the stack, the command switch will allocate an available IP address for it automatically. Through the command switch, the network management station implements management and maintenance over various member switches.

9.1.2 Stack Management of Quidview Device Manager

As a feature of the Quidview Device Manager, stack management primarily provides functions in the following two aspects:

I. Stack management and maintenance

It is mainly used for stack maintenance and operation, including creating a stack, opening a stack, browsing device information of the stack, configuring stack protocols, configuring stack VLAN, browsing and configuring stack ports, etc.

II. Auxiliary functions

The auxiliary functions include displaying stack device list, refreshing stack, identifying stack ports, deleting stack, etc.

9.2 Managing and Maintaining the Stack

9.2.1 Creating a Stack

After the Quidview Device Manager starts, open the device serves as the stack main switch, click the “+” on the “Stack Management” node in the function navigation pane and then double-click the unfolded “New Stack” node; the system pops up the [New Stack] dialog box, as shown in Figure 9-1:

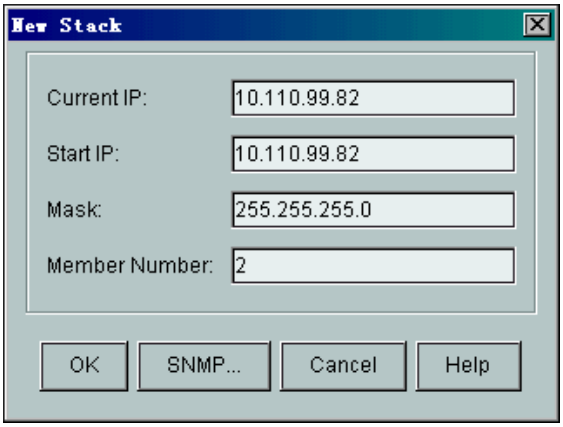


Figure 9-1 New Stack

After inputting proper parameters, click <OK> to create a stack. The meaning of various parameters in the dialog box is listed in Table 9-1:

Table 9-1 Parameters in the [New Stack] dialog box

Parameter	Description
Current IP	Current IP address of the command switch of the stack
Start IP	The start IP address of the IP pool when the stack is created
Mask	The mask of stack’s IP pool
Member Number	The number of switches that can be included in the stack

9.2.2 Opening a Stack

After the Quidview Device Manager starts, select [Device/Open Device…] menu item or click the button on the toolbar. In the popup [Open Device] dialog box, enter the IP address of the command switch of the stack to open the panel of the stack, as shown in Figure 9-2.

Note:

If you enter the IP address of a member switch of the stack in the [Open Device] dialog box, the [Whether to open the stack] dialog box will pop up. Here click <OK>, and you will also open the panel of the corresponding stack. In this case, the member switches should be connected to NMS. Otherwise, the stack cannot be opened.

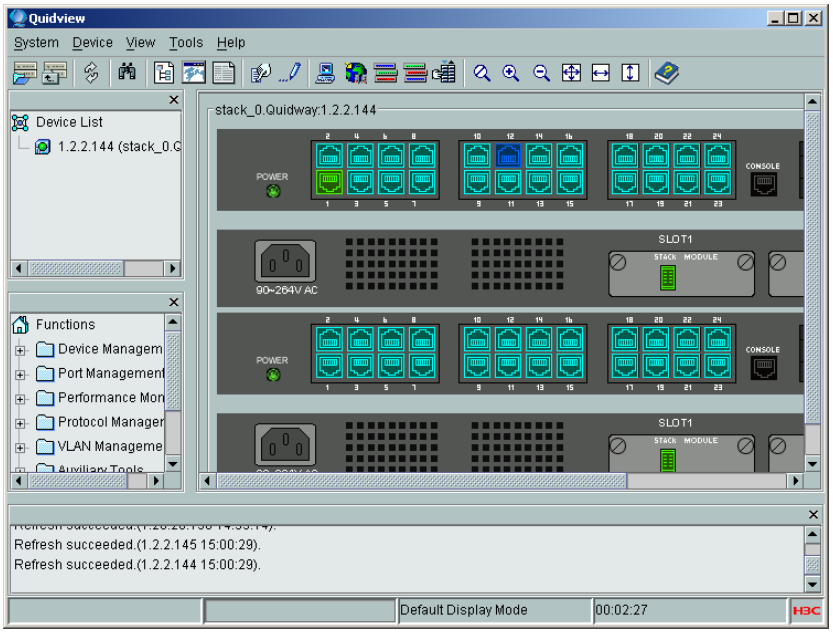


Figure 9-2 Device panel view of the stack

The system information browsing and configuration function of the stack is used to browse and configure the device system information of the switches in the stack. The traffic monitor function is used to monitor the traffic of the main switch in the stack. For the operation procedures and parameter meanings of the two functions, refer to the device management and performance monitor part in *Quidview Device Manager User Manual Volume I*.

9.2.3 Configuring Stack Protocols

I. Configuring stack GARP

It configures the global GARP of various switches in the stack. For the detailed operation and parameter description, refer to section 5.3.1 "Configuring Global GARP".

II. Configuring stack port GARP

It configures GARP for each switch port in the stack. For the detailed operation and parameter operation, refer to section 5.3.2 "Configuring Port GARP".

III. Configuring stack RSTP

It configures the global RSTP of various switches in the stack. For the detailed operation and parameter description, refer to section 5.2.1 "Configuring the RSTP of a Device".

IV. Configuring port STP of the stack

It configures the port STP of various switches in the stack. For the detailed operation and parameter description, refer to section 5.2.2 "Configuring Port RSTP".

🕮 **Note:**

Protocol configuration is performed on all the switches of a stack.

9.2.4 Configuring Stack VLAN

Like the VLAN configuration for single device, the VLAN configuration for stack includes VLAN management, VLAN virtual interface management, VLAN Trunk management and adding port to VLAN. There is no essential difference between them, except that the VLAN configuration of single device only addresses one device whereas the VLAN configuration of stack addresses all switches in the stack.

For the detailed operations of parameter description, refer to Chapter 4 "VLAN Configuration".

9.2.5 Browsing and Configuring Stack Port

The port browsing and configuration of stack and that of a single device are different only in the objects they address. The former addresses all switches in the stack, whereas the latter addresses a single device.

For the detailed operations of parameter description, refer to Chapter 3 "Port Management".

9.2.6 Stack Member List

In Figure 9-2, double-click on [Stack Management/Device List] node in the function window to open the [Device List] dialog box, which displays the list of all the devices in the stack.

9.2.7 Identifying Stack Port

In Figure 9-2, you can double-click on [Display Mode/Stack Display Mode] node in the function window and switch between identifying and not identifying the stack port in the device panel.

9.2.8 Deleting a Stack

In Figure 9-2, double-click on [Stack Management/Delete Stack] node in the function window to open the confirmation dialog box. Click <OK> in the dialog box so as to delete the existent stack.

Chapter 10 QoS Management

10.1 QoS Overview

10.1.1 ACL

A series matching rules need configuring for the network devices to identify the packets to be filtered. After identifying the packets, the switch can permit or deny them to pass through according to the defined policy. Access Control List (ACL) is used to implement such functions.

An ACL consists of three factors, traffic rule, flow action, and time range. A traffic rule defines which traffic matches the ACL. Flow action decides how to process the matching traffic, either permit or deny. Time range specifies when the matching traffic will be processed with the corresponding flow action. The traffic matching the flow rule of an ACL will be permitted or denied during the specified time range.

ACL classifies the data packets with a series of matching rules, including source address, destination address and port number, etc. ACL is deployed on the switch ports. The switch checks the data packets with the conditions in ACL and determines to forward or discard them.

10.1.2 What is QoS

With the rapid development of computer network, more and more requirements have been arising. More and more important real time data such as voice and image, which are sensitive at bandwidth, delay, and jitter are transmitted over the network. Accordingly, the issue of how to guarantee the Quality of Service is put forward. One approach to solve this problem is to increase the bandwidth, which can only buffer it to a certain degree, because the bandwidth is limited and costly. Another approach, which is also more effective, is to manage the network traffic by means of congestion management, congestion avoidance, and traffic shaping.

Quality of Service (QoS) is to provide services of different qualities on demands for the traffic traveling on different networks (such as LAN, frame relay, and IP network). QoS provides the following functions:

- Bandwidth reservation

The bandwidth reservation is to reserve a minimum bandwidth for the specified traffic accessing a switch, so that some QoS requirements such as packet loss rate, delay, and jittering, can be met even when the network congestion occurs.

- Traffic policing

In order to deliver better service with the limited network resources, QoS polices the traffic of the specific users on the ingress, so that they can make a better use of the assigned resource.

- Port rate limit

The port rate limit is the port-based line rate used for limiting the general speed of packet output on the port.

- Traffic Redirect

You can specify a new port to forward the packets according to your requirements on the QoS policy.

- Traffic priority

The Ethernet switch can deliver traffic priority service for some special packets. The tags include TOS, DSCP and 802.1p, etc., which can be used and defined in different QoS models respectively.

- Selecting egress queue for the packets

The Ethernet switch can select corresponding egress queues for special packets.

- Queue scheduling

Queue scheduling is commonly used to resolve the problem that multiple messages compete with resource when the network congestion happens. Here we introduce three kinds of queue scheduling algorithms with respective features, Strict-Priority Queue (SP), Weighted Round Robin (WRR) and Delay Bounded WRR.

- Mirrored To

The Mirrored To function is to copy the specified data packets to the CPU for network diagnosis and troubleshooting.

- Port mirroring

The port mirroring function is to copy the specified data packets to the observing port for network diagnosis and troubleshooting.

- Flow-based traffic statistics

With the flow-based traffic statistics, you can count and analyze the packets at your requirements.

10.1.3 QoS of Quidview Device Manager

The QoS of Quidview Device Manager mainly includes time range configuration maintenance, ACL configuration maintenance, and QoS configuration maintenance. The configurations and parameters are introduced in details respectively.

Note:

The QoS configuration of S3505 is taken as an example in this chapter. Some parameters of QoS configuration may vary with the type of device. For details, see the device-specific user manual.

10.2 Time-Range Configuration

The time-range configuration is to provide the related configuration (such as ACL) with the support based on time-range. The major functions are to configure and maintain the time-range rule and decide whether a time point is contained in a specified time-range.

The time-range configurations include the methods to organize and apply the time-ranges. Every time-range rule has a unique name and contains multiple absolute and periodic time-ranges as its sub-items. For absolute time-range configuration, a time-range is specified in the yyyy-mm-dd, hh:mm format. The periodic time-range is a weekly range specified in the hh-mm format.

If a time-range consists of multiple absolute and periodic time-ranges, the final range is the intersection of the absolute time-range combination and the periodic time-range combination. Quidview Device Manager can be configured with up to 256 time-ranges.

10.2.1 Adding a Time-Range

After the Quidview Device Manager starts, select [Device/Open Device…] or click on the toolbar to open an Ethernet switch which supports QoS. Click "+" on [QoS Management] node and double-click the [QoS Management] leaf in the expanded node. The [QoS Management] dialog box pops up, shown as the following figure.

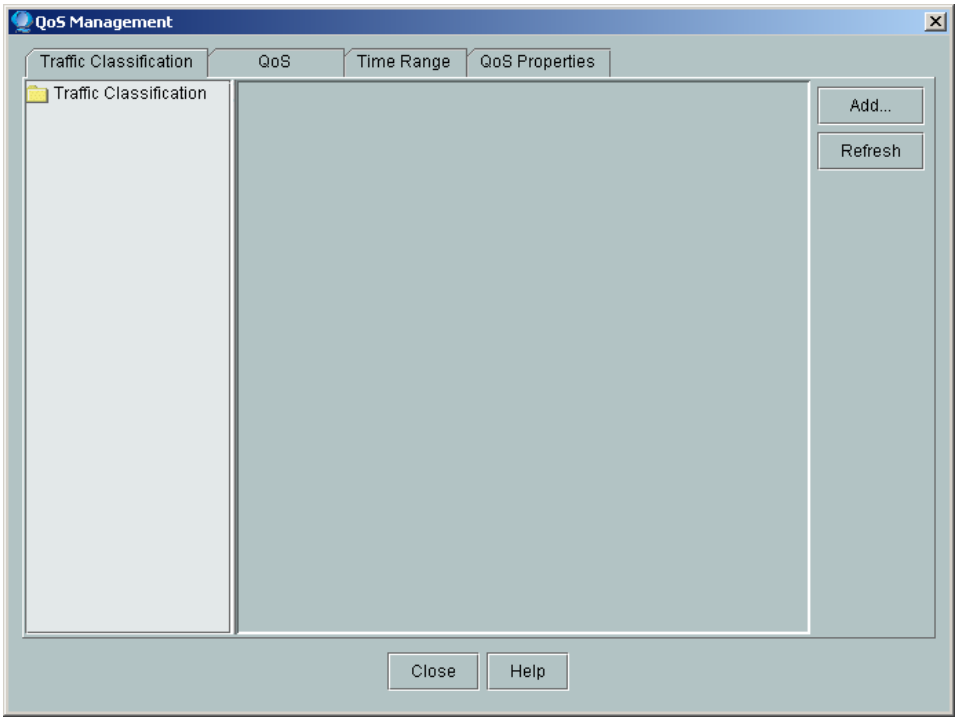


Figure 10-1 QoS Management

Click the [Time Range] tab and double-click the [Time Range] node in the window on the left. Then you will find the time range management dialog box, shown as the following figure.

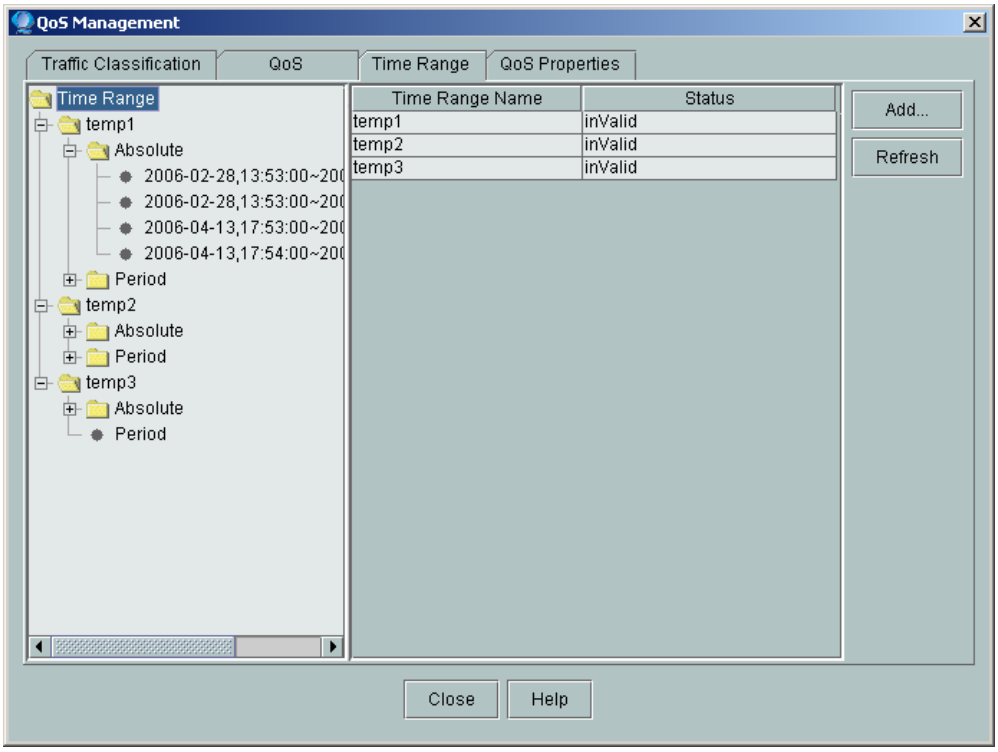


Figure 10-2 Time range management

Click <Add...> on the right column and the [Add a Time Range] dialog box appears. You can input or select a time range in the combo box. If you input a new time range name, you can click <Finish> to add it directly.

If you select an existing time range, you need to select the type and click <Next> to configure the specific start time and end time.

As shown in Figure 10-3, the [Add an Absolute Time Range] dialog box allows you to either input the time range in the edit box or select the start time and end time of an absolute time range by clicking ... . Then, click <Finish> to complete the configurations of the time range.

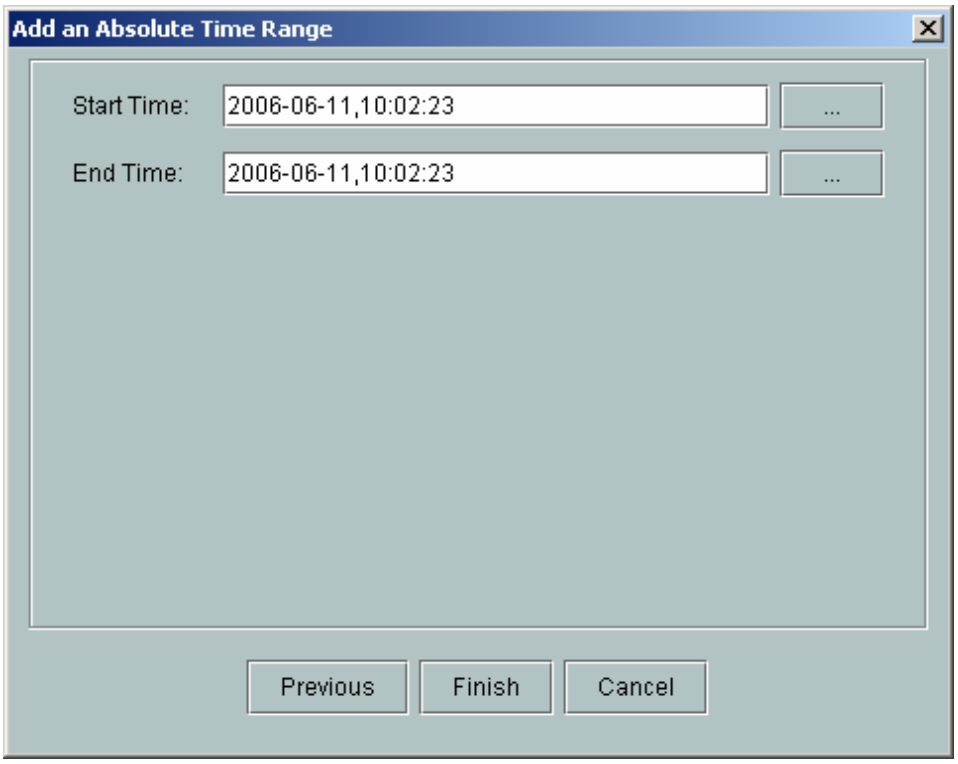


Figure 10-3 Adding an absolute time range

As shown in Figure 10-4, the [Add a Periodic Time Range] dialog box allows you to input the start time and end time in the edit boxes and select on which day of the week the time range takes effect. Click <Finish> to complete the configurations of the time range.

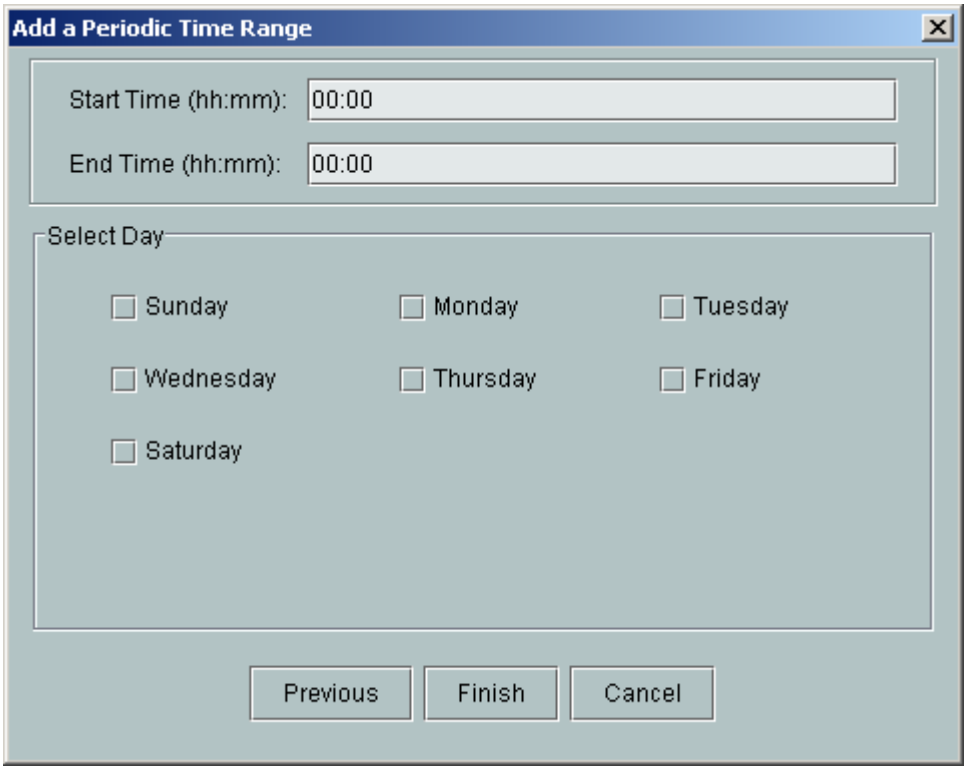


Figure 10-4 Adding a periodic time range

Caution:

- If the start time and end time are unspecified, the time range covers the whole day.
- If no end time is specified, the time range ends at the latest time as the system can display.
- If a time-range consists of multiple absolute and periodic time-ranges, the final range is the intersection of the absolute time-range combination and the periodic time-range combination.

10.2.2 Deleting a Time Range

In the time range management dialog box as shown in Figure 10-2, select a configured time range and click <Delete>. The system pops up a prompt for confirmation. Click <OK> to delete an existing time range.

10.3 ACL Configuration

The Ethernet switches have the following ACLs:

- Standard ACL
- Extended ACL
- Layer-2 ACL

Among them, every type of ACL can be further divided into numbered and named ACLs. So there are six types of ACLs in an Ethernet switch.

Each type of ACL will be introduced in the following sections respectively.

10.3.1 Adding a Standard ACL

Click the [Traffic Classification] tab in the [QoS management] dialog box as shown in Figure 10-1. Click <Add...> in the right column and see the [Type Selection Window] dialog box. In the combo box, select "standard ACL" and click <Next>. The [Add Standard ACL] dialog box will pop up, as shown in the following figure.

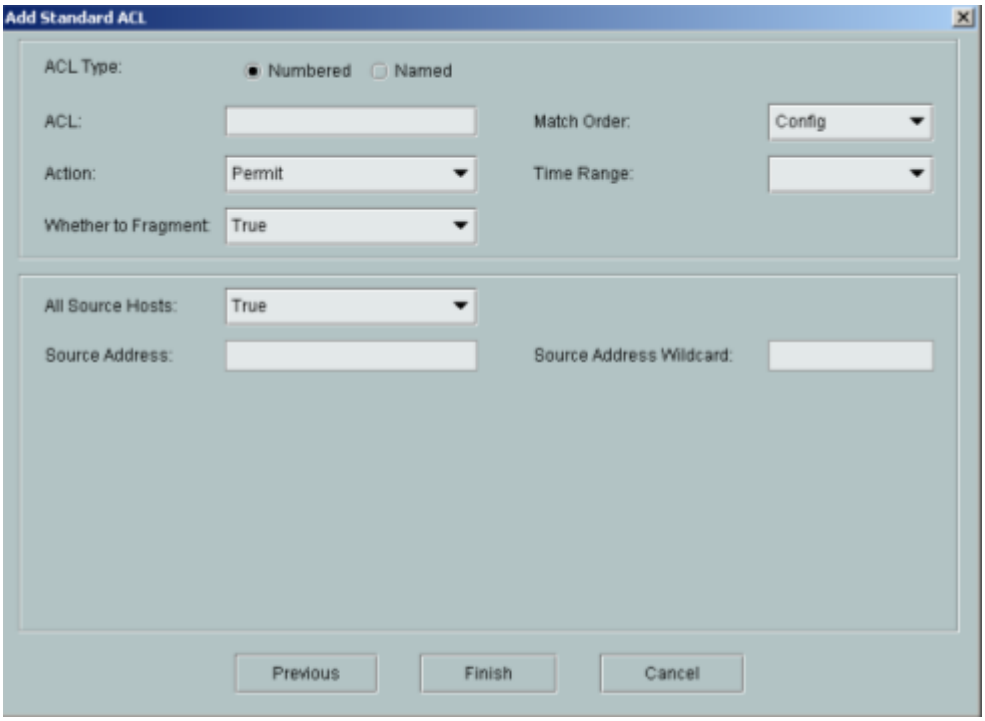


Figure 10-5 Adding Standard ACL

This dialog box allows you to create a standard ACL. The parameters are explained as follows:

- ACL Type: Numbered and named ACLs;
- ACL: Specify the ACL sequence number or name; For a numbered ACL, the parameter represents the ACL sequence number; for a named ACL, the parameter specifies an ACL name with a character string beginning with an English letter (i.e. [a-z, A-Z]) and excluding space and quotation marks. The ACL name is not case-sensitive. The **all** and **any** keywords cannot be used as a name.

- Match Order: "Config" means to follow the configuration order; "Auto" means to follow the depth-first order;
- Action: Set the match actions. "permit" will let the matching packets through, while "deny" does not let any matching packets through;
- Time Range: (Optional) Specify when an ACL takes effect. If the parameter is omitted, the ACL will always take effect.
- Whether to Fragment: "True" means the rule takes effect on the fragmented packets but ignores those not fragmented. "False" means the rule takes effect on all the packets;
- Source Address: Source IP address in dotted decimal notation.
- Source Address Wildcard: Source address wildcard in dotted decimal notation, such as 0.0.255.255;

10.3.2 Adding an Extended ACL

In the combo box of the [Type Selection Window] dialog box, select "Extended ACL" and click <Next>. The [Add Extended ACL] dialog box will pop up, as shown in Figure 10-6.

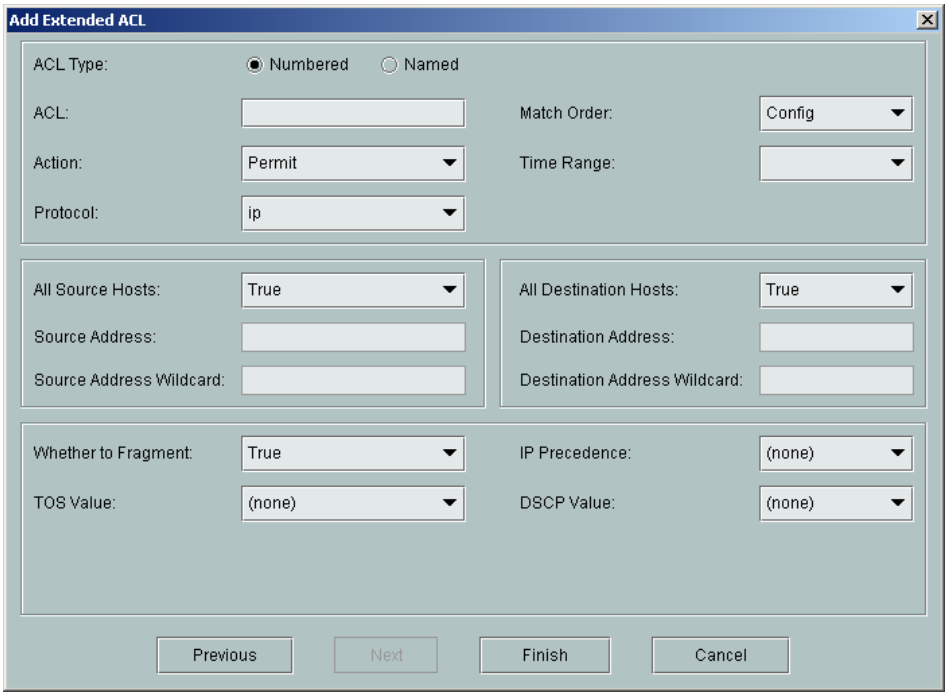


Figure 10-6 Adding Extended ACL

In the above dialog box, the user creates an extended ACL. Only the special parameters in it are introduced here. For the parameters the same as those of the standard ACL, refer to section 10.3.1 “Adding a Standard ACL”.

- Protocol: Specify the protocol in use. The protocol can be icmp, igmp, tcp, udp, ip, gre, ospf, and ipinip. IP represents all the protocols of IP suite;

- Destination Address: Destination IP address in dotted decimal notation.
- Destination Address Wildcard: Destination address wildcard in dotted decimal notation;
- IP Precedence: (Optional) An integer ranging from 0 to 7. The values in descending order represent respectively: network, internet, critical, flash-override, flash, immediate, priority, and routine.
- TOS Value: (Optional) The packets can be classified based on the ToS value;
- DSCP Value: (Optional) The packets can be classified based on the DSCP value.

10.3.3 Adding a Layer-2 ACL

Select "L2 ACL" and click <Next> in the [Type Selection Window] dialog box. The [Add L2 ACL] dialog box shown as Figure 10-7 will pop up.

In this dialog box, a user creates a L2 ACL. Only the special parameters in it are introduced here. For the parameters same as those of the standard ACL, refer to the preceding descriptions.

- Protocol: (Optional) Specify the protocol carried by the Ethernet frame for an ACL.
- 802.1 Priority: Specify 802.1p;
- VLAN Label: Configure to match the data packets with VLAN label or not;
- Encapsulation Type: Specify the encapsulation format at link layer for an ACL;
- All Source Hosts: Specify the information about the source hosts of the data packet for an ACL. "True" means the rule takes effect on all the hosts; "False" requires further host information settings including "source MAC address" and "source MAC address wildcard";
- Source Interface: Set source interface information about a data packet;
- Source MAC Address: Specify the source host MAC address information of the data packets for an ACL;
- Source MAC Wildcard: Specify the source MAC addresses interesting the users with the source MAC parameter. For example "source MAC wildcard" can be 0.0.ffff and indicate that a user only cares about the first 32 bits of the source MAC address (or the 0 bits);
- All Destination Hosts: Specify the information about the destination hosts of the data packet for an ACL. "True" means the rule takes effect on all the hosts; "False" requires further host information settings including "destination MAC address" and "destination MAC address wildcard";
- Destination Interface: Specify the destination interface of the data packets for an ACL.
- Destination MAC: Specify the destination host MAC address of the data packets for an ACL;
- Destination MAC Wildcard: Specify the destination MAC addresses interesting the users with the destination MAC parameter. For example "source MAC wildcard"

can be 0.0.ffff and indicate that a user only cares about the first 32 bits of the source MAC address (or the 0 bits);

- Source VLAN ID: Specify the source VLAN of the data packet for an ACL;
- Destination VLAN ID: Specify the destination VLAN of the data packet for an ACL.

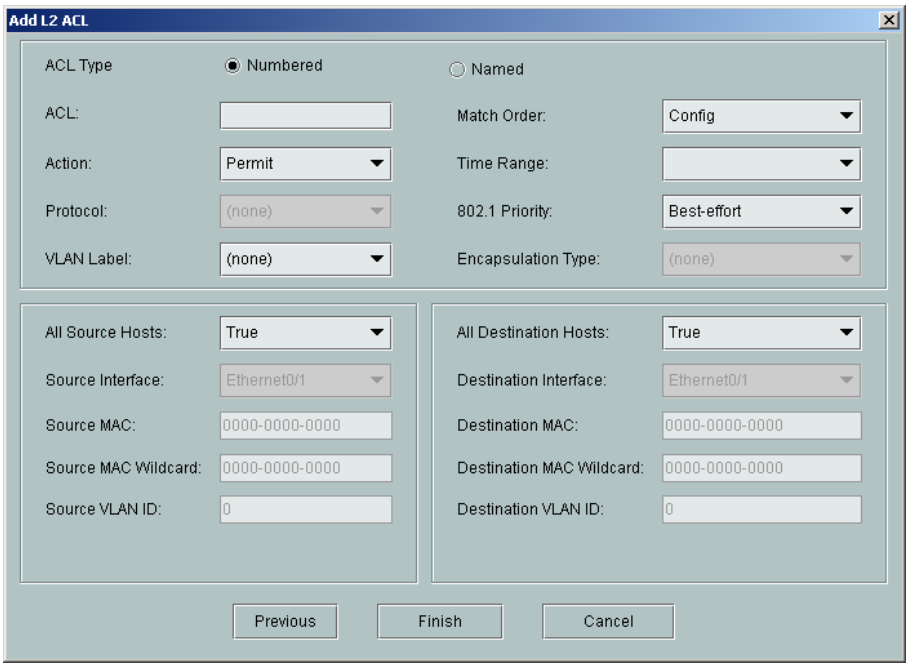


Figure 10-7 Adding L2 ACL

10.3.4 Deleting an ACL

In the ACL management interface, select a configured ACL and click <Delete>. In the popped up prompt dialog box, click <OK> for confirmation and delete the ACL from the system.

10.4 QoS Configuration

Ethernet Switch Series support the following QoS features: traffic limit, traffic priority, queue scheduling, Mirrored To, traffic statistics and packet filtering.

10.4.1 Traffic Limit

The traffic limit is on the flow basis for monitoring the traffic rate. It takes corresponding actions to deal with the flow at exceeding rate, such as discarding or lowering the priority.

In the [QoS Management] dialog box shown as Figure 10-8, click the [QoS] tab to display the QoS management interface, shown as the following figure.

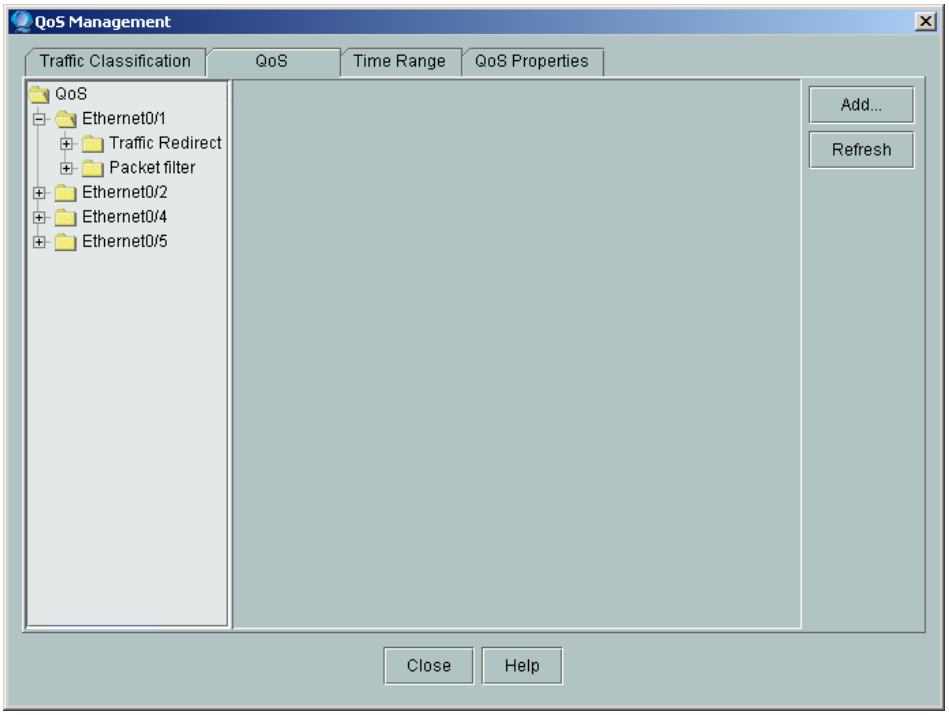


Figure 10-8 QoS Management

Click <Add...> and the [Select Port] dialog box will pop up. Select a port, and click <Next> to enter the [Select ACL] dialog box, as shown in Figure 10-9.

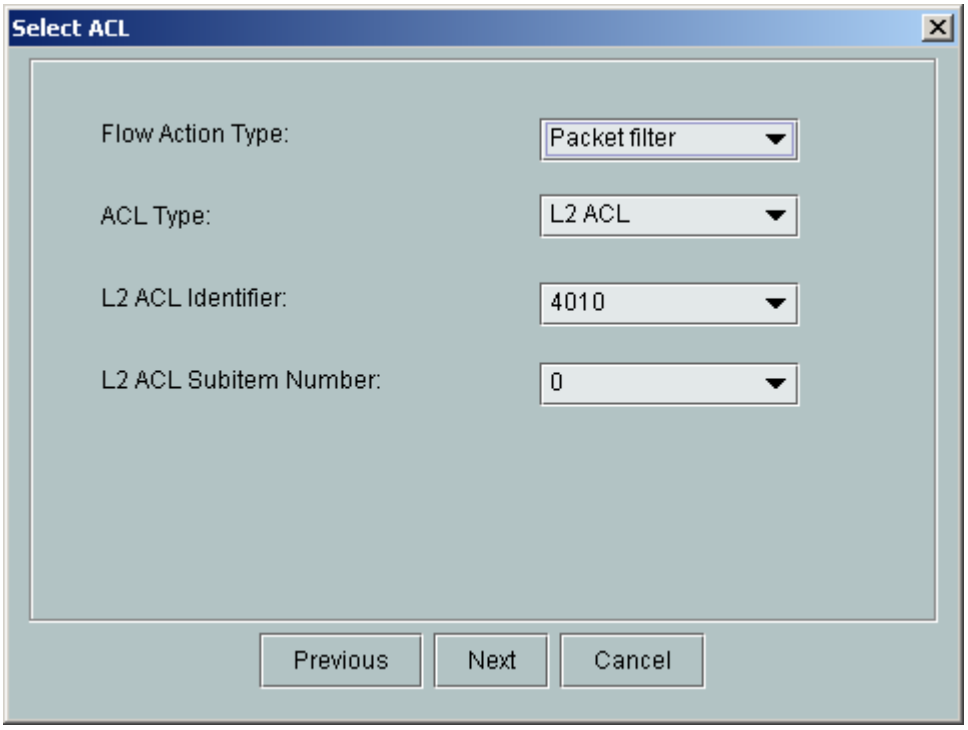


Figure 10-9 Select ACL

Select a defined ACL and set "Flow Action Type" to “Traffic Limit”. Click <Next> and the [Add Traffic Limit] dialog box will pop up. Set the committed information rate, committed burst size, excess burst size and peak information size, and choose the actions applied when rate is exceeded and not exceeded. Then, click <Finish> and you can add a traffic limit.

10.4.2 Traffic Priority

In the [Select ACL] dialog box shown as Figure 10-9, set the “Flow Action Type” to "Traffic Priority" and select a configured ACL. Click <Next> and the [Add Traffic Priority] dialog box pops up, as shown in Figure 10-10.

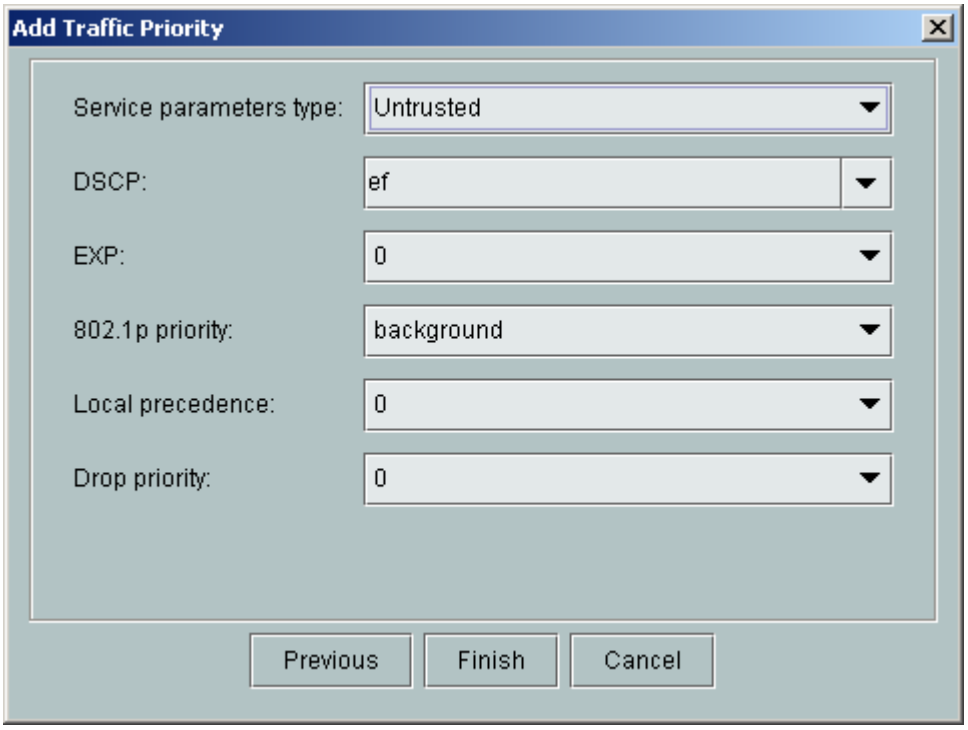


Figure 10-10 Add Traffic Priority

Configure the parameters related to the traffic priority in the above interface and click <Finish> to add a traffic priority.

10.4.3 Traffic Redirect

Packet Traffic Redirect is to redirect the packets to be forwarded to CPU or a specified output port.

In the dialog box shown as Figure 10-9, set the “Flow Action Type” to "Traffic Redirect" and select a configured ACL. Click <Next> and the [Add Traffic Redirect] dialog box pops up, as shown in Figure 10-11.

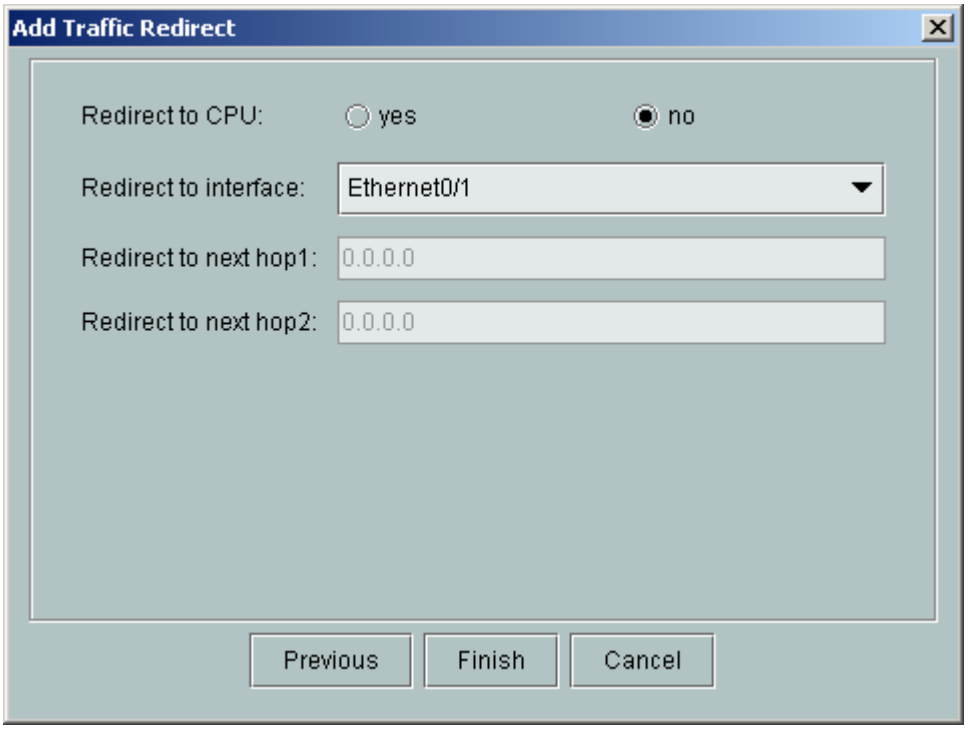


Figure 10-11 Add Traffic Redirect

After configuring to redirect the packets to CPU or a port, click <Finish> to add a traffic redirect entry.

10.4.4 Traffic Statistics

Traffic statistics is used for counting the data packets of the specified traffic. It counts the data information of the data packets forwarded by a switch and matching some defined ACL.

In the dialog box shown as Figure 10-9, set the “Flow Action Type” to "Traffic Statistic" and select a configured ACL. Click <Finish> to complete the operation.

10.4.5 Mirrored To

The function of Mirrored To is to copy the traffic matching ACL rule to the CPU to analyze and monitor the packets.

In the dialog box shown as Figure 10-9, set the “Flow Action Type” to "Mirrored To" and select a configured ACL. Click <Next> to display the [Add Mirrored To] dialog box. Choose whether to copy the traffic matching ACL rules to CPU and click <Finish>.

10.4.6 Packet Filtering

Packet filtering refers to apply a certain ACL on a specified interface.

Choose “Packet filter” from the [Flow Action Type] drop-down list shown in Figure 10-9, and select a defined ACL. Then, click <Finish> to complete the packet filtering configuration.

10.4.7 Configuring and Deleting QoS Items

In the [QoS Management] dialog box shown as Figure 10-8, select a configured QoS item, click <Delete> or <Configure…> to delete a QoS item or configure it. For the parameters in the configuration dialog box, refer to the preceding description.

10.5 QoS Properties

Select the [QoS Properties] tab in the [QoS Management] dialog box. The tab page for configuring QoS properties appears, as shown in Figure 10-12.

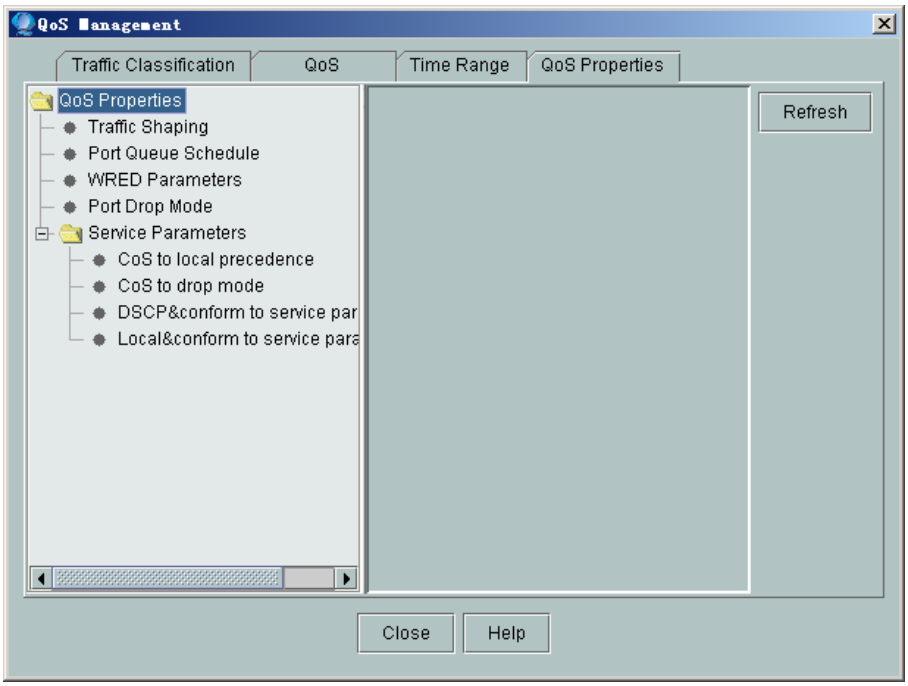


Figure 10-12 Configuring QoS properties

Traffic Shaping

Traffic shaping is used to control the transmission rate of outbound packets. It ensures that the packets are transmitted at an even rate that goes well with the downstream devices, so as to reduce packet loss or congestion. It differs from Traffic policing mainly in two: it buffers the packets transmitted at rates beyond the limit to achieve the even transmission, but the latter simply discards those packets; it increases delay, but the latter does not.

The switch supports both port-based traffic shaping and queue-based traffic shaping. If port-based, the traffic shaping concerns all the traffic of the selected port; if

queue-based, it concerns only the specified queue of the port. To configure any of the two, choose the appropriate parameters.

Double-click the [QoS Properties/Traffic Shaping] node in the tab page for configuring QoS properties. The dialog box shown in Figure 10-13 is displayed.

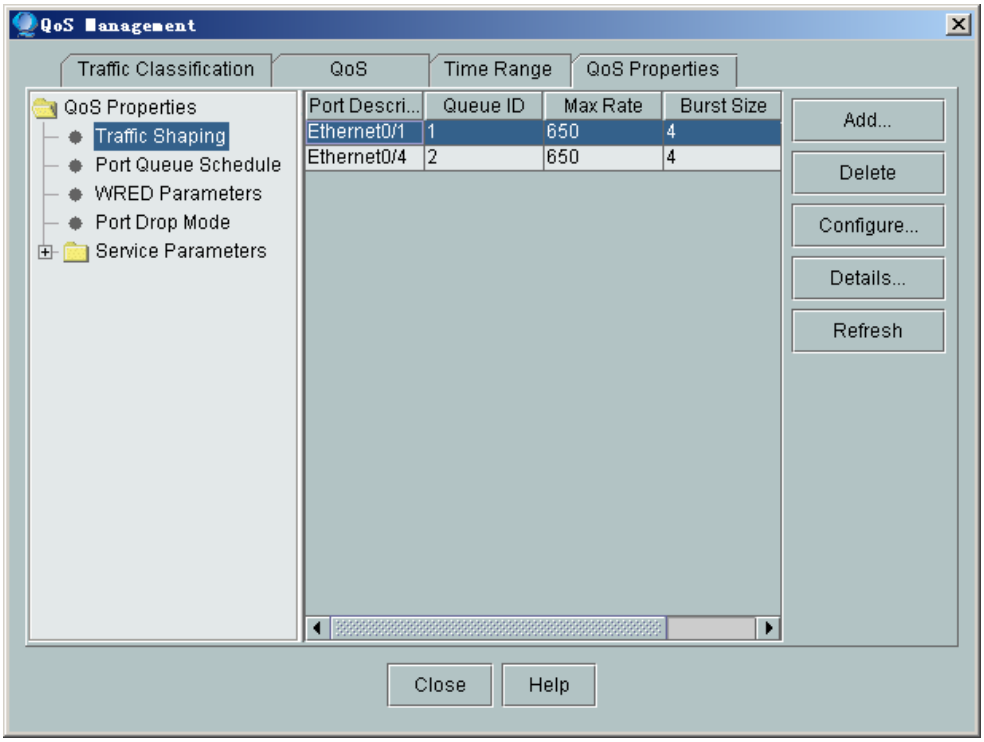


Figure 10-13 Traffic shaping

This dialog box shows such details of traffic shaping as:

- Port Description: Description on the port where traffic shaping is applied to
- Queue ID: Queue ID of the port where traffic shaping is applied to
- Max Rate: Ranges from 650 Kbps to 10600000 Kbps. Its value must be a multiple of 650 for low-speed links, yet a multiple of 41500 for high-speed links.
- Burst Size: Burst size for traffic shaping, measured in Bytes.

I. Add

Click <Add…>, and the [Add Traffic Shaping] dialog box appears. You can configure traffic shaping parameters as needed, including port description, queue ID, max traffic rate, burst size and buffer limit.

II. Configure

Select a row in the list, and click <Configure…>. The user can configure the max traffic rate, burst size and buffer limit by necessity in the displayed box.

III. Detailed information

Select a row in the list, and click <Details…> or double-click the row. The related details are displayed.

IV. Delete

Select one or more rows in the list, and click <Delete>. The selected traffic shaping information is deleted.

10.5.1 Port Queue Schedule

Each switch port supports eight output queues. When receiving a packet, the switch puts it into an appropriate output queue by its local precedence. Under network congestion, queue schedule is used to solve the contrast between multiple packets and limited resources. The switch supports both SP (Strict-Priority) and WRR (Weighted Round Robin) queue schedule algorithms, which can be separately adopted by different output queues. Therefore, the switch can have three schedule modes:

- SP schedule for all queues;
- WRP schedule for all queues: Output queues are grouped by necessity into WRP high-priority queues and WRP low-priority queues. Schedule goes in turn: in the high-priority queues first, then shifting to the low-priority ones when no packet waits in high-priority queues. By default, all queues are in WRP low-priority group.
- SP schedule for part of queues and WRP schedule for the other part: Each part adopts the appropriate schedule mode to pick out one queue from each of the SP schedule group, WRP high-priority schedule group and WRP low-priority schedule group. Then the system schedules these three queues by strict priority.

Double-click the [QoS Properties/Port Queue Schedule] node in the tab page for configuring QoS properties. The dialog box shown in Figure 10-14 is displayed.

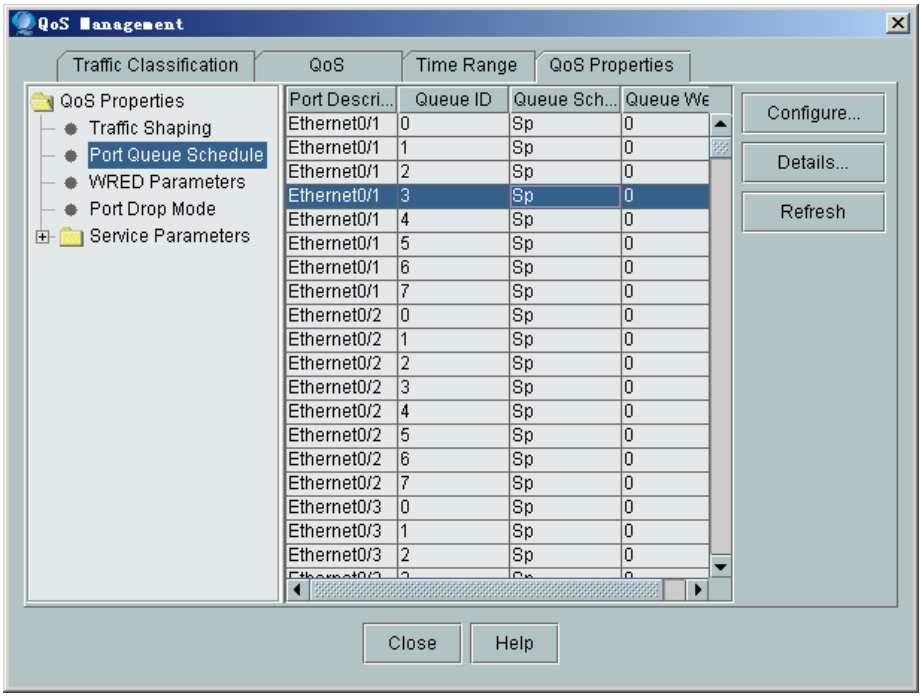


Figure 10-14 Port queue scheduling

This box contains such detailed information of port queue schedule as:

- Port Description: Description on the port where port queue schedule is applied to
- Queue ID: Queue ID of the port, in the range of 0 to 7.
- Queue Schedule Mode: There are three queue schedule modes of Sp, Wrr high priority, and Wrr low priority.
- Queue weight: Weight of the queue, ranging from 0 to 255.

To configure a schedule mode, select the appropriate row from the list and click <Configure…>. Choose the queue schedule mode among SP, WRR high priority, and WRR low priority; and set the queue weight.

10.5.2 WRED Parameters

When receiving a packet, the switch assigns it a conform level, or in other words, colors it. There are three conform levels: 0 for red, 1 for yellow, and 2 for green. Once congestion occurs, the switch will drop packets (the red first, and the green last) as soon as possible to release the otherwise occupied queue resources, and keep the packets from those high-delay queues to relax it.

Parameters to avoid congestion and threshold of dropping can be configured by queue and conform level.

The switch supports two kinds of dropping algorithms:

- Tail drop: Dropping threshold can be separately set for different queues. Once the number of red, yellow, or green packets exceeds the appropriate buffer lower limit, the system starts dropping the packets lining after the lower limit.
- Random detect: When dropping packets by queue, the system takes the dropping level into account. Once the number of red, yellow, or green packets exceeds the appropriate buffer lower limit, the system starts dropping the packets that line between the buffer lower limit and the buffer upper limit by a slope. Once the number of red, yellow, or green packets exceeds the appropriate buffer upper limit, the system starts dropping the packets that line after the upper limit.

Before configuring the dropping algorithm on the switch, you need to configure the WRED parameters of the output queues of each port first.

The switch provides four sets of default WRED parameters, respectively represented by WRED index 0, 1, 2, and 3. Each set contains 80 parameters, with ten for every of the eight ports. The user can tailor the current WRED parameters to detailed requirements.

Double-click the [QoS Properties/WRED Parameters] node in the tab page for configuring QoS properties. The dialog box shown in Figure 10-15 is displayed.

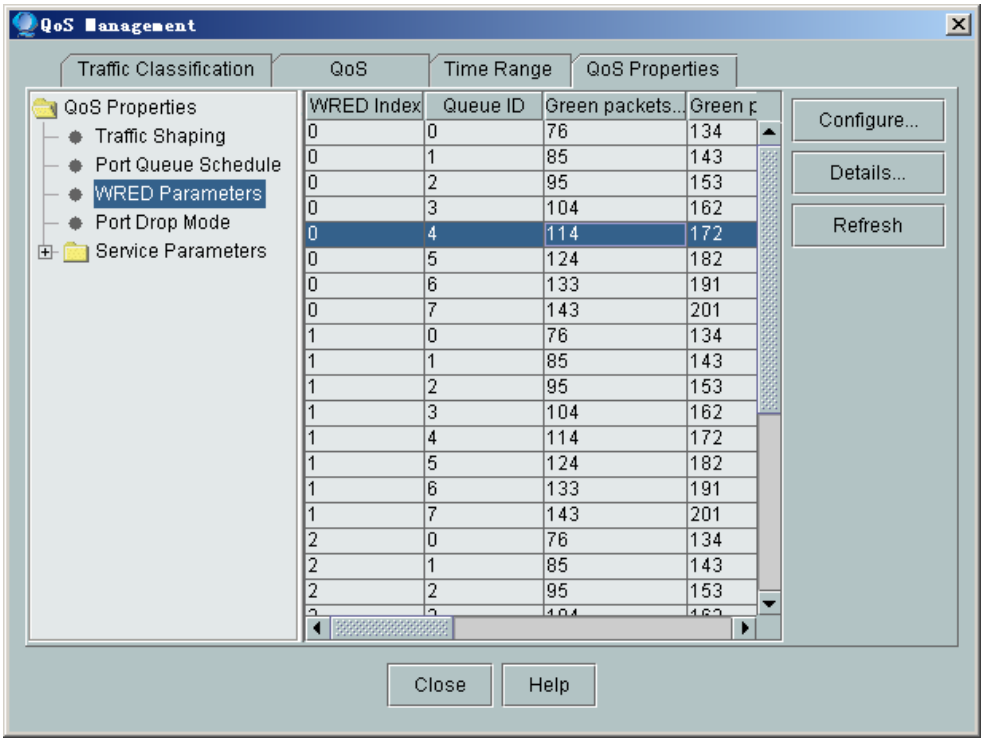


Figure 10-15 Configuring WRED parameters

This box contains such detailed information of WRED parameters as:

- WRED index
- Queue ID

- Green packets buffer lower limit: Queue length for the green packets to be randomly discarded.
- Green packets buffer upper limit: Queue length for the green packets to be totally discarded.
- Green packets max drop probability: Maximum drop probability of green packets.
- Yellow packets buffer lower limit: Queue length for the yellow packets to be randomly discarded.
- Yellow packets buffer upper limit: Queue length for the yellow packets to be totally discarded.
- Yellow packets max drop probability: Maximum drop probability of yellow packets.
- Red packets buffer lower limit: Queue length for the red packets to be randomly discarded.
- Red packets buffer upper limit: Queue length for the yellow packets to be totally discarded.
- Red packets max drop probability: Maximum drop probability of red packets.
- Average buffer length weight: Weight of the average queue length.

Select a row in the list and click <Configure…>. Specify each entry box as required and click <OK> to complete the configuration.

Select a row in the list and click <Details…>; or double-click the row. The related details are displayed.

⚠ **Caution:**

Attention must be paid when configuring WERD parameters, which have great influence on the forwarding capability of the system.

10.5.3 Port Drop Mode

Before configuring the dropping algorithm on the switch, you need to configure the WRED parameters of the output queues of each port first. For the WRED parameter configuration, refer to section 10.5.2 “WRED Parameters”.

Double-click the [QoS Properties/Port Drop Mode] node in the tab page for configuring QoS properties. The dialog box shown in Figure 10-16 is displayed.

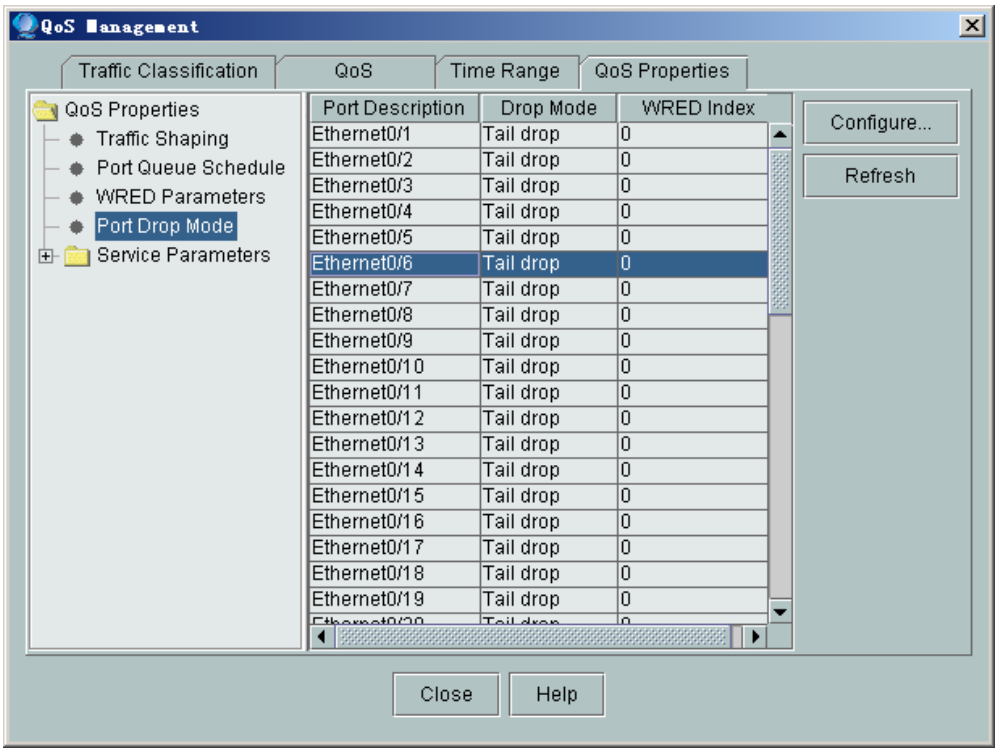


Figure 10-16 Managing port drop mode

This box shows the details of drop modes of the device ports, including:

- Port Description
- Drop mode: Random detect or Tail drop
- WRED index

Select a row in the list and click <Configure…>. The user can configure the drop mode of the selected port as necessary. If Random detect is chosen, WRED parameters need to be configured. Click <OK> when you finish the configuration.

Double-click a row in the list and the related details are displayed.

10.5.4 Service Parameters

The switch has a set of QoS-specific parameters, including 802.1p precedence (CoS), DSCP precedence, local precedence (the local meaning precedence the switch assigns to packets) and conform level (referred to when dropping packets, thereby also named drop precedence).

I. Mapping of COS to Local Precedence/Drop Mode

After receiving a packet, the switch assigns it a set of service parameters by certain rules. At first, the switch looks up the "CoS->Drop-precedence" and "CoS ->Local-precedence" mapping tables to get the conform level and local precedence of the packet according to its CoS. The switch has provided default values for the mapping tables, but users are allowed to tailor them to their specific requirements. If a

packet fails to get a local precedence, the switch borrows the default local precedence of the receiving port.

1) Mapping of CoS to Local Precedence

In the tab page for configuring QoS properties, double-click the [QoS Properties/Service Parameters/CoS to local precedence] node in the function pane. The dialog box shown in Figure 10-17 is displayed.

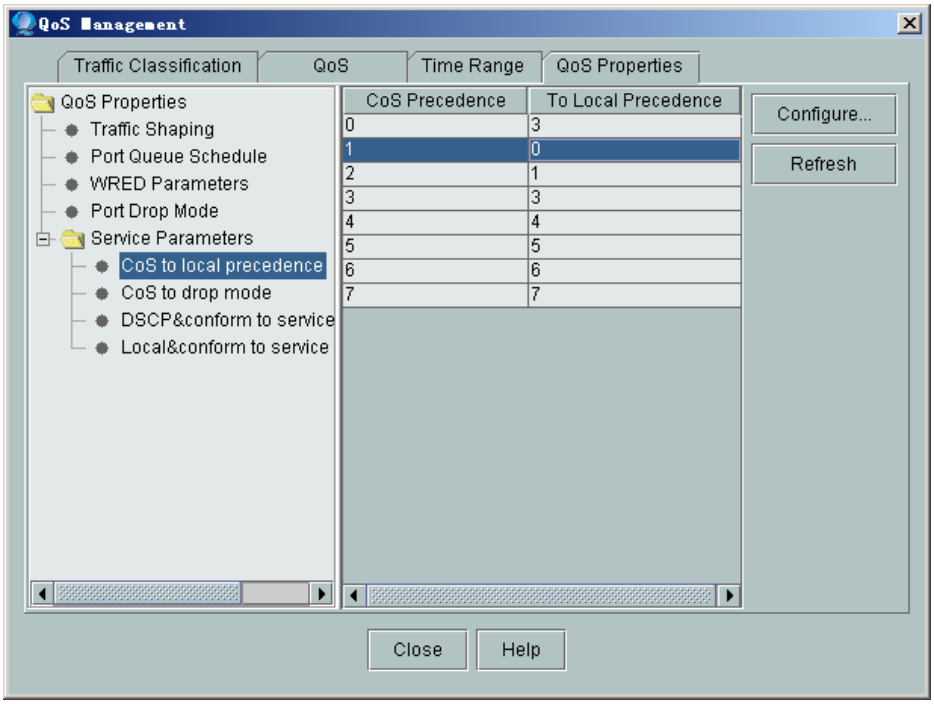


Figure 10-17 Mapping of CoS to local precedence

This box contains a mapping list of COS to local precedence.

Select a row in the list and click <Configure…>. The [Config CoS to local precedence] dialog box is displayed. Choose in the drop-down list the local precedence that CoS will map to. Then click <OK> to complete this operation.

2) Mapping of CoS to Drop Mode

In the tab page for configuring QoS properties, double-click the [QoS Properties/Service Parameters/CoS to drop mode] node in the function pane. The dialog box shown in Figure 10-18 is displayed.

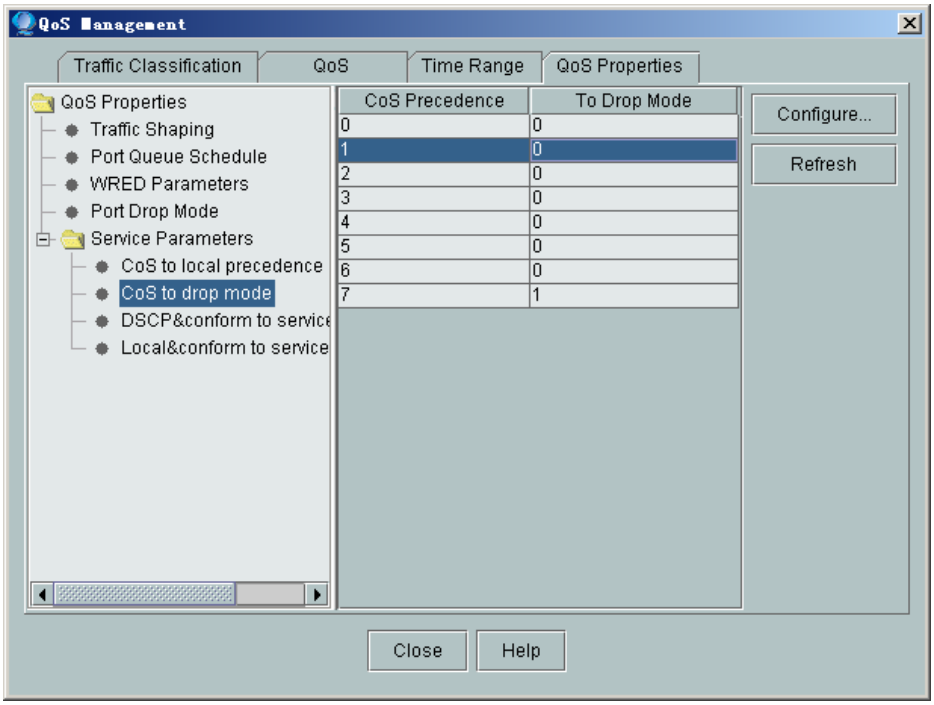


Figure 10-18 Mapping of CoS to drop mode

This dialog box contains a mapping list of CoS to drop mode.

Select a row in the list and click <Configure…>. The [Config CoS to drop mode] dialog box is displayed. Choose in the drop-down list the drop mode that CoS will map to. Then click <OK> to complete this operation.

II. Service Parameter Configuration for Traffic Policing

Traffic policing is a kind of traffic-based rate control. With it, the switch will discard the superfluous packets or reset the service parameters once the traffic exceeds predefined specifications.

Traffic policing involves the reset of service parameters by the "DSCP + Conform-Level->Service parameters" mapping table, and the reallocation of 802.1p precedence by the "Local-precedence + Conform-Level->CoS" mapping table. Users are therefore encouraged to configure these two tables or use the default table values based on actual situation.

1) Mapping of DSCP + Conform-level to Service Parameters

Double-click the [QoS Properties/Service Parameters/DSCP&conform to service parameters] node in the function pane. A dialog box shown in Figure 10-19 is displayed.

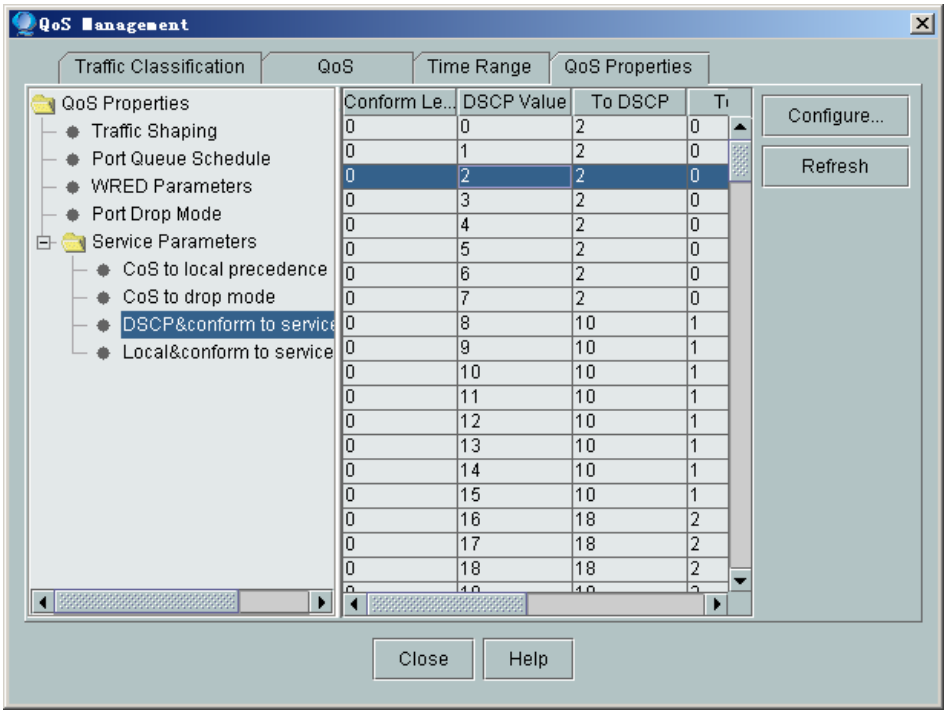


Figure 10-19 Mapping of DSCP&conform to service parameters

This dialog box shows a mapping list of “DSCP + conform-level” to service parameters.

Select a row and click <Configure…>. The [Config DSCP & conform to service parameters] dialog box is displayed.

The [Config DSCP&conform to service parameters] dialog box lists:

- Conform level: Cannot be configured.
- DSCP value: Cannot be configured.
- To DSCP: DSCP value that “DSCP + conform-level” is mapped to
- To EXP: EXP value that “DSCP + conform-level” is mapped to
- To CoS: CoS value that “DSCP + conform-level” is mapped to
- To local precedence: Local precedence that “DSCP + conform-level” is mapped to
- To drop mode: Drop mode that “DSCP + conform-level” is mapped to

Click <OK> to complete the configuration.

2) Mapping of Local-precedence + Conform-level to CoS

Double-click the [QoS Properties/Service Parameters/Local&conform to service parameters] node in the function pane. A dialog box shown in Figure 10-20 is displayed.

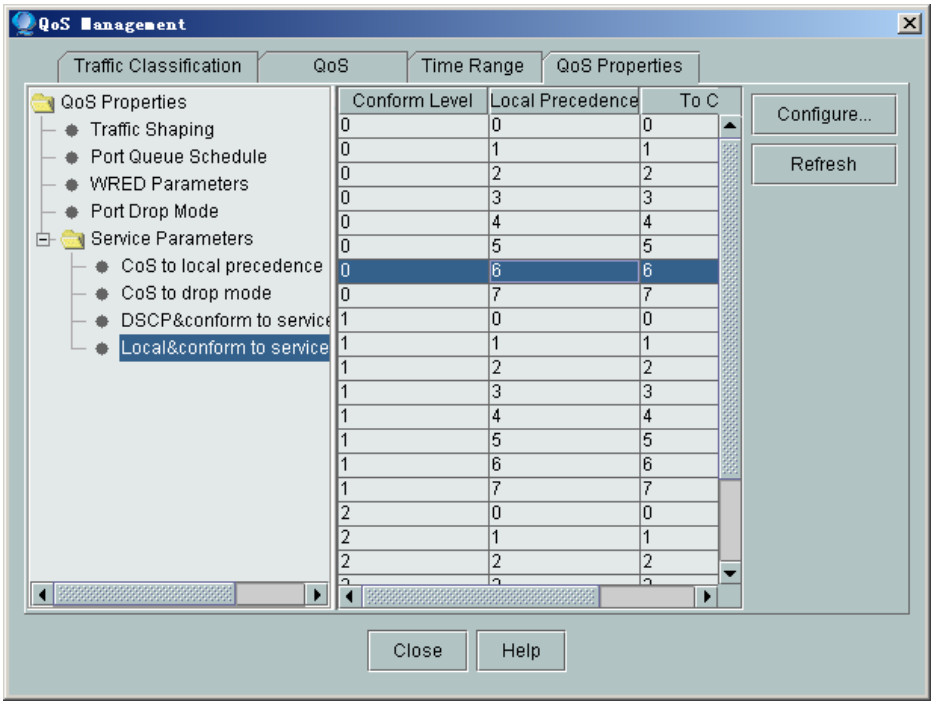


Figure 10-20 Mapping of local&conform to CoS

This box shows a mapping list of “local-precedence + conform-level” to CoS.

Select a row in the list and click <Configure…>. The [Config Local&conform to service parameters] dialog box is displayed.

The [Config Local&conform to service parameters] dialog box lists:

- Conform Level: Ranges from 0 to 2.
- Local Precedence: Ranges from 0 to 7.
- To CoS: CoS value that “local-precedence + conform-level” is mapped to. It ranges from 0 to 7.

Click <OK> to complete this operation.

Chapter 11 WLAN Management

11.1 Overview

This chapter contains information on how to configure, manage and monitor your Access Point (AP) device on a real-time basis through Wireless Local Area Network (WLAN) management. AP devices act as bridges between wireless networks and cable networks to provide wireless access for WLAN terminal users.

11.2 Configuration Parameters Management

11.2.1 System Attributes Management

Start Quidview Device Manager, select [Device/Open…] from the menu or click on the toolbar to display the panel view of your WLAN device, click <Configuration Parameters> in the function navigation window and the [Configuration Parameters] dialog box appears.

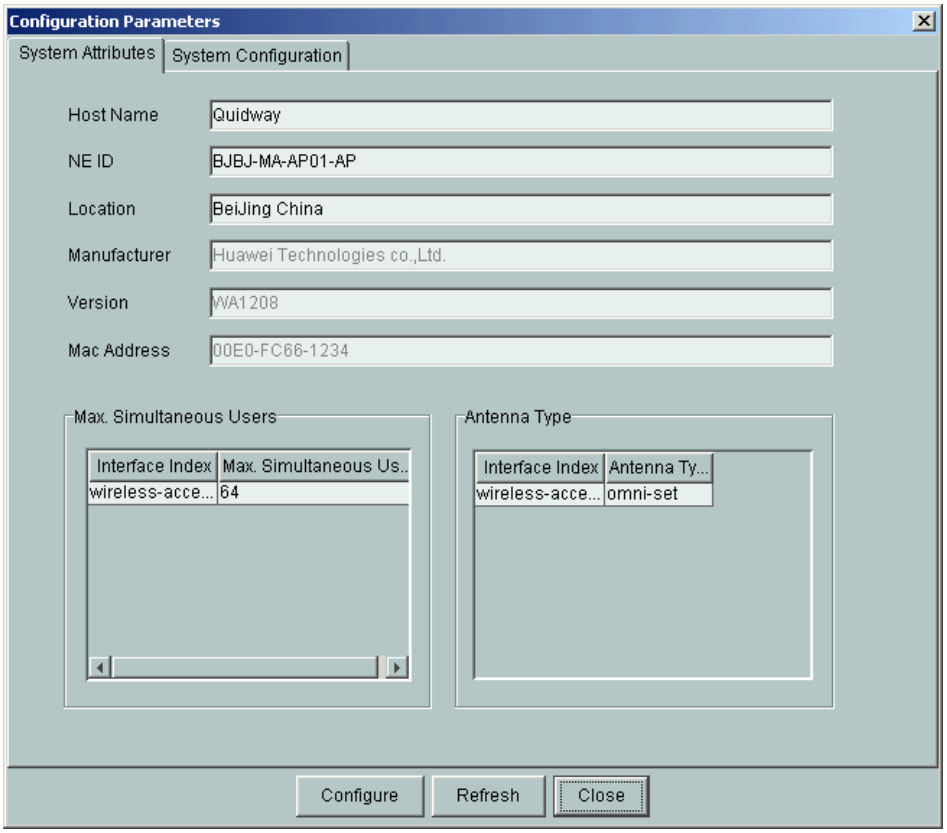


Figure 11-1 Configuration parameters – System Attributes

The dialog box displays system attributes of your AP device, including Host Name, NE ID, Location, Manufacturer, Version, MAC Address, Max. Simultaneous Users (by port) and Antenna Type.

Max. Simultaneous Users refers to the maximum number of users that can access the port at the same time. Its value ranges from 0 to 64.

Antenna types include omni-set, sector-get, dual-slant-sector, two-sector-set and others.

In this dialog box, you can configure Host Name, NE ID and Location, but not the other attributes. Click <Configure…> to save your configuration.

11.2.2 System Configuration Management

Start Quidview Device Manager, select [Device/Open…] from the menu or click on the toolbar to display the panel view of your WLAN device, click <Configuration Parameters Management> in the function navigation window and the [Configuration Parameters] dialog box appears. Select the [System Configuration] tab where you can browse and configure the system information of your AP device.

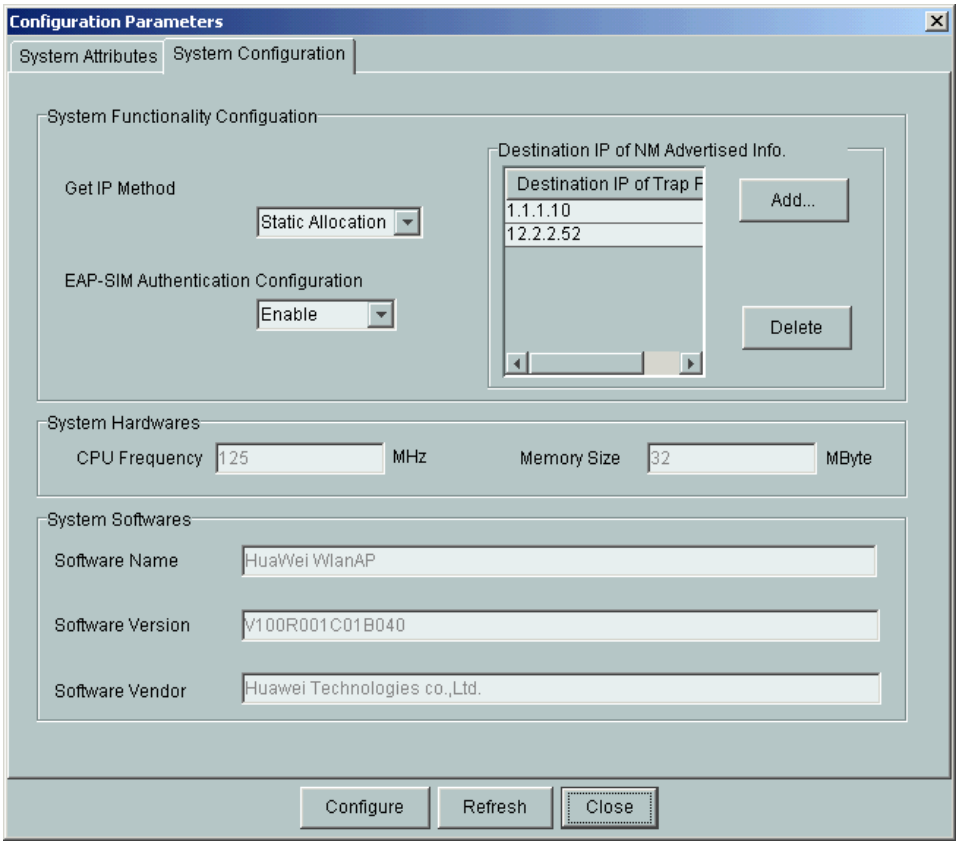


Figure 11-2 Configuration parameters – System Configuration

This dialog box displays the following system configuration information of your AP device: Get IP Method, EAP-SIM Authentication Configuration, CPU Frequency, Memory Size, Software Name, Software Version and Software Vendor.

The Get IP Method includes three options: Static Allocation, DHCP and BOOTH. You can select one from the drop-down list box.

There are three options for EAP-SIM Authentication Configuration: Enable, Disable and Not Support. Select one option from the drop-down list box.

Destination IP of NM Advertised Info refers to the Destination IP of Trap Packets. AP device supports multiple destination IP addresses of NM advertised information. Click <Add> or <Delete> to add or the delete destination IP addresses of Trap packets.

Note:

- With WA 1208, you can Click <Add> or <Delete> to add or delete destination IP addresses of NM advertised information; but with WA 1006E that only has a fixed number of destination IP addresses, you can only click <Modify> to change the addresses.
- 0.0.0.0 indicates that the address is not being used.

11.3 Site Configuration Management

Start Quidview Device Manager, select [Device/Open…] from the menu or click on the toolbar to display the panel view of your WLAN device, click <Site Configuration> in the function navigation window and the [Station Management] dialog box appears.

11.3.1 Information Management

In the [Station Management] dialog box, select the Info. Management tab. Then the [Info. Management] interface appears, as shown in the following figure:

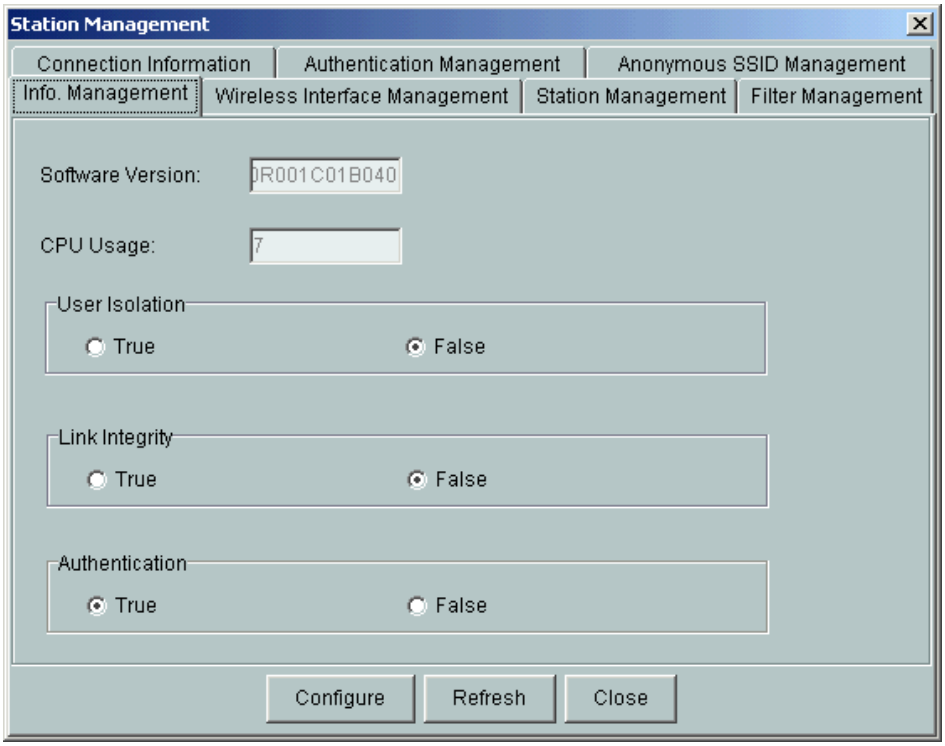


Figure 11-3 Info Management

This dialog box displays information of your AP device on software version, CPU usage, user isolation, link integrity and authentication.

11.3.2 Wireless Interface Management

In the [Station Management] dialog box, click the [Wireless Interface Management] tab. Then the [Wireless Interface Management] interface appears as shown in the following figure:

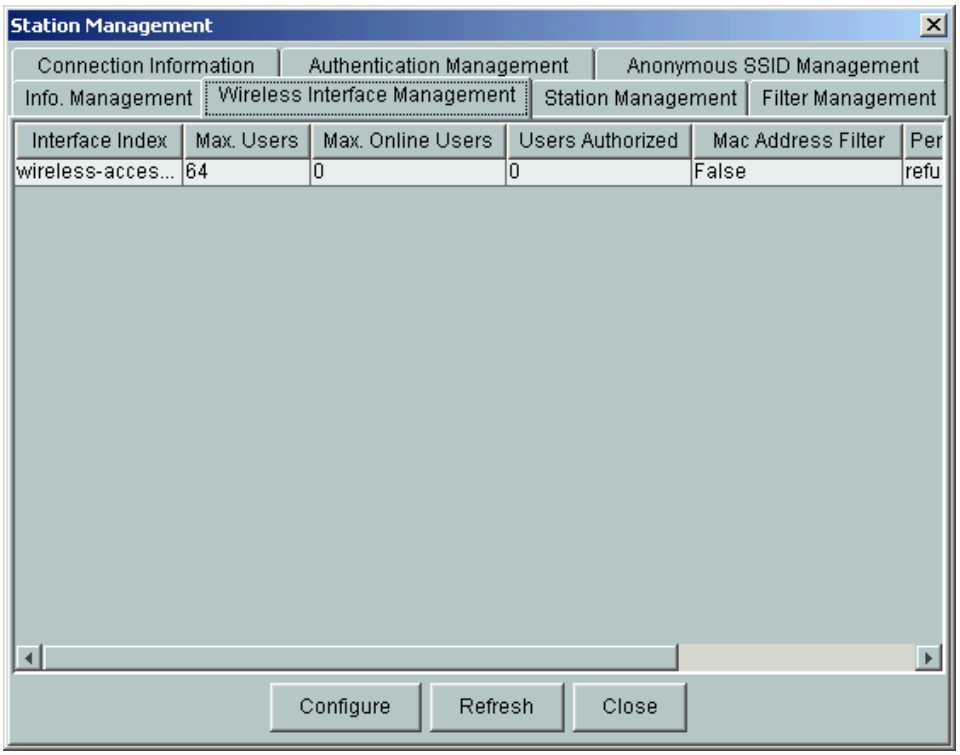


Figure 11-4 Wireless Interface Management

This dialog box displays each port's Max. Users, Max. Online Users, Users Authorized, MAC Address Filter, Permit/Deny, Anonymous SSID, Access Upper Protocol Stack.

Related configuration on WA1208 allows or inhibits STA (station, i.e. wireless access user device) to access WA1208 upper protocol. If STA is allowed to access WA1208 upper protocol, then you have one more way to operate and maintain WA1208 besides serial port access and Telnet.

11.3.3 Station Management

In the [Station Management] dialog box, select the [Station Management] tab. Then the [Station Management] interface appears as shown in the following figure:

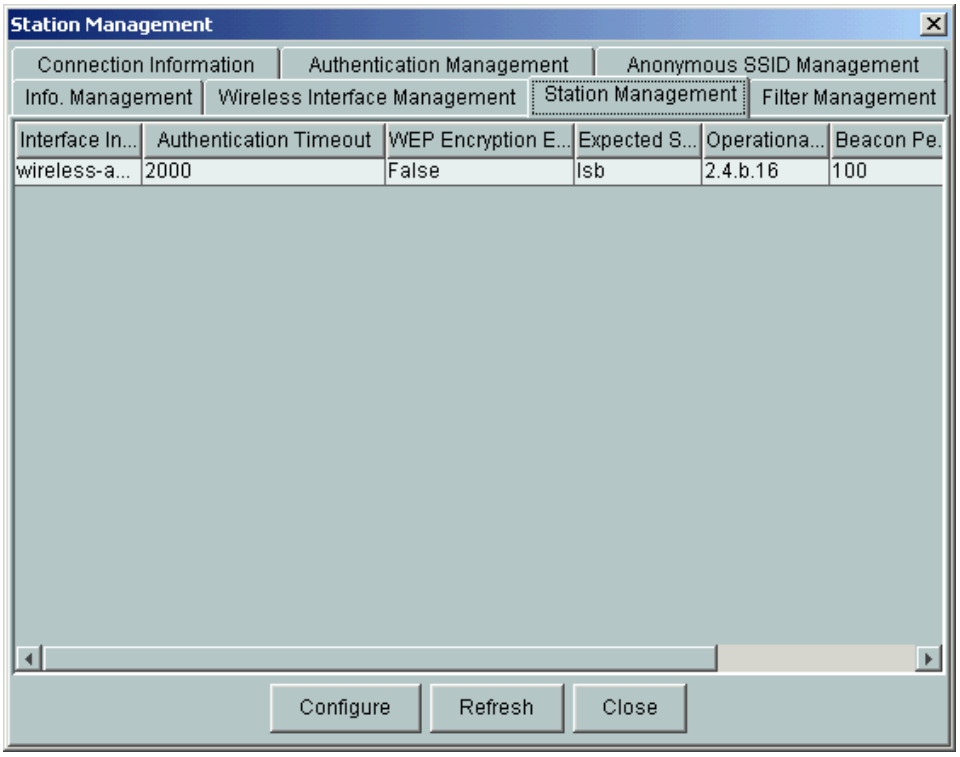


Figure 11-5 Station Management

The dialog box displays information on Authentication Timeout, WEP Encryption Enable, Expected SSID, Operational Rate Set, Beacon Period, DTIM period and Connection Timeout.

AP devices periodically send beacon packets which connect the AP device with other access point devices or network control devices to indicate the existence of the AP device. The period that AP devices send beacon packets is called beacon period. Beacon time ranges from 20 to 1000. The default value is 100.

Delivery Traffic Indication Map (DTIM) refers to the number of beacons used to wake up the wireless devices in the energy-saving mode. The DTIM period specifies the time interval between beacon packets (in milliseconds).

11.3.4 Filter Management

In the [Station Management] dialog box, select the [Filter Management] tab, then the [Filter Management] interface appears as shown in the following figure.

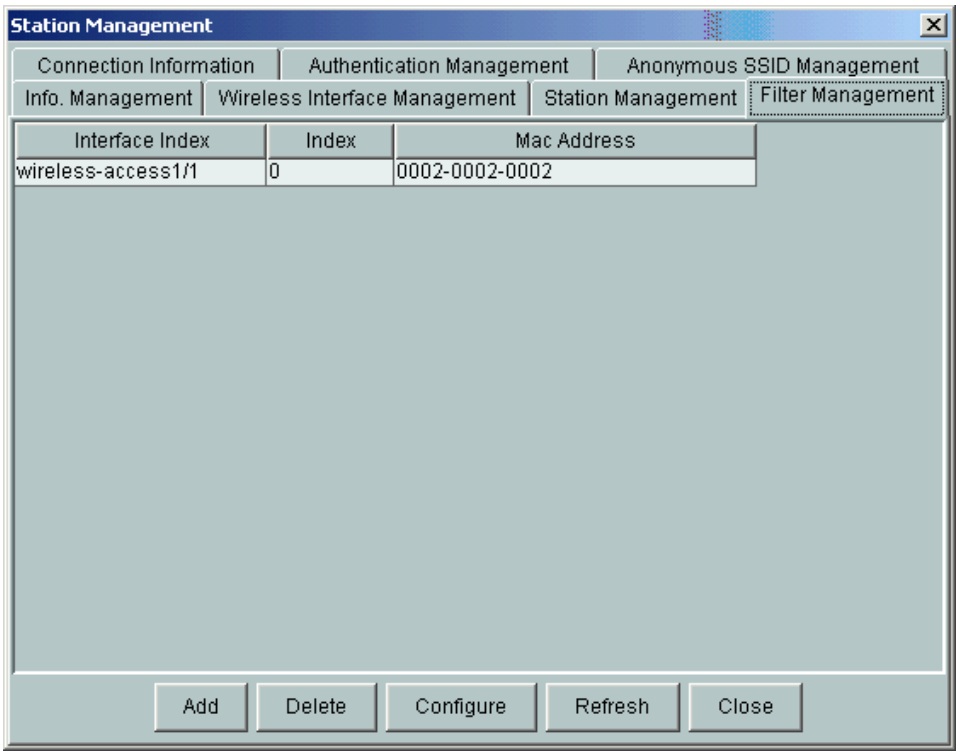


Figure 11-6 Filter Management

This dialog box displays the MAC addresses of some devices that are not authorized to access the ports of your AP device.

Click <Add>, and the [Add Filtered MAC Address] dialog box appears. Input a certain valid MAC address; click <Add> to finish the operation. This will inhibit the user of this MAC address to access the port of your AP device.

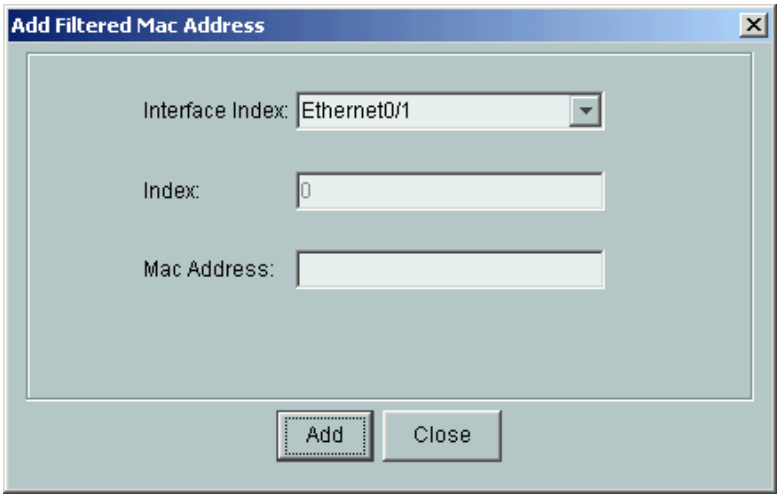


Figure 11-7 Add Filtered MAC Address

11.3.5 Connection Information

Select the Connection Information tab in the [Station Management] dialog box, then the [Connection Information] interface appears as shown in the following figure.

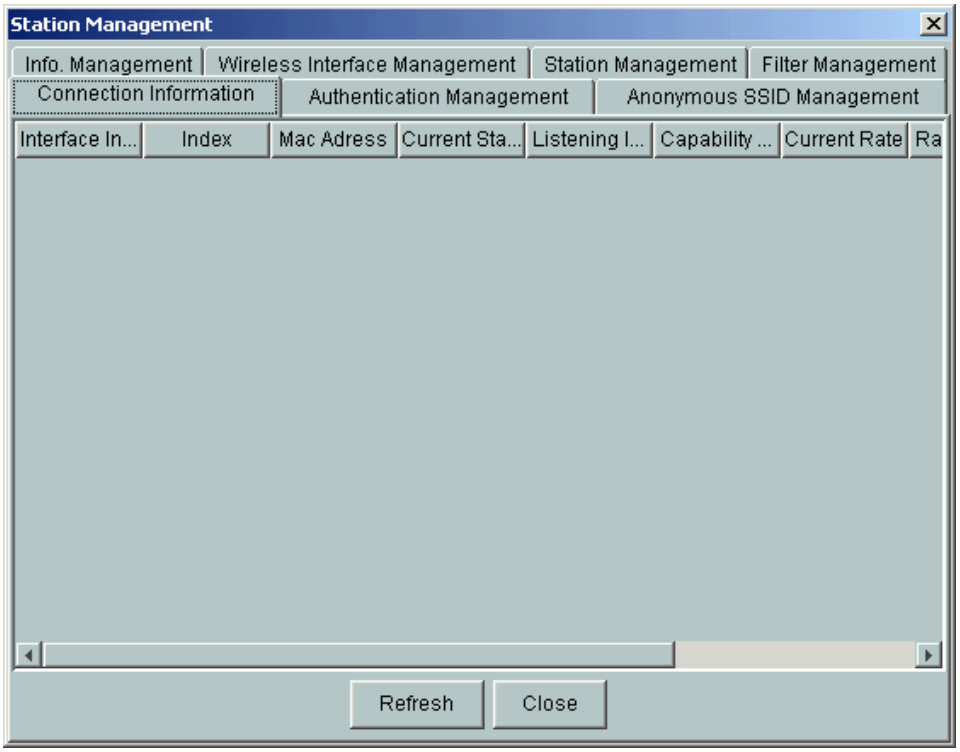


Figure 11-8 Connection Information

This dialog box displays information on connected terminals: MAC Address, Current Status, Listening Interval, Capability Set, Current Rate, Rate Sets Supported, Rate Set and Failure Count.

11.3.6 Authentication Management

In the [Station Management] dialog box, select the Authentication Management tab. Then the [Authentication Management] interface appears, as shown in Figure 11-9.

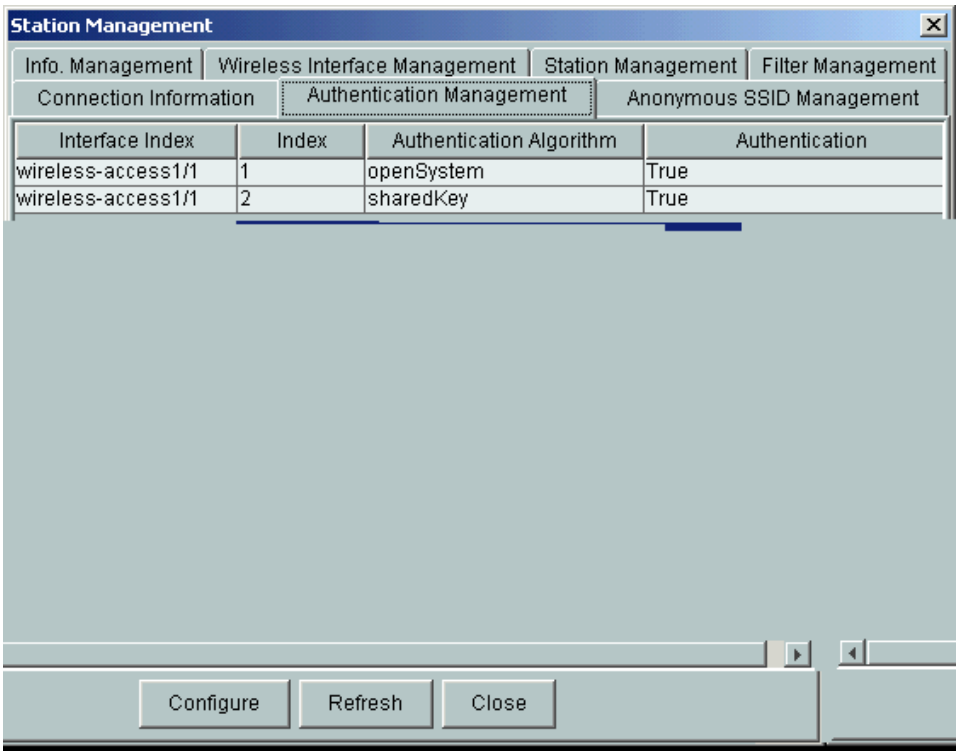


Figure 11-9 Authentication Management

The dialog box displays each AP port's authentication algorithm and whether they support true authentication.

Select one from the Interface Index that you want to reconfigure, click <Configure…>. There are two types of algorithms: open system and shared key.

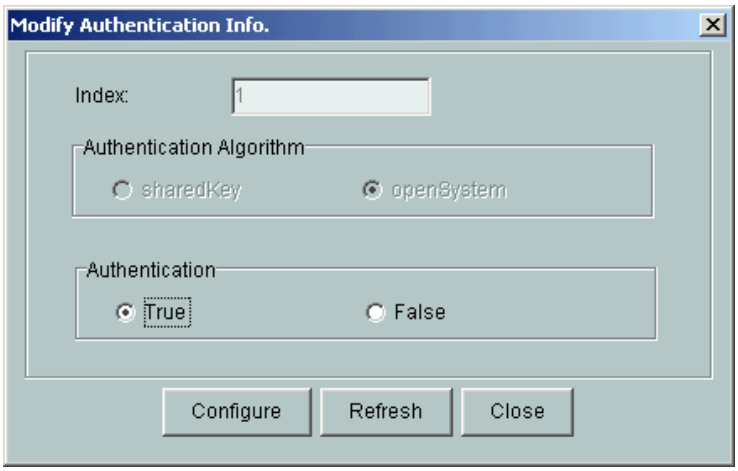


Figure 11-10 Modify Authentication Info

11.3.7 Anonymous SSID Management

You need to set up an SSID (Service Set ID) in both your AP device and its connected device (like a wireless network card) to access WLAN through WA1208. If WA1208 supports SSID access, then you need to configure an anonymous SSID table.

In the [Station Management] dialog box, select the [Anonymous SSID Management] tab. Then the [Anonymous SSID Management] interface appears as shown in the following figure.

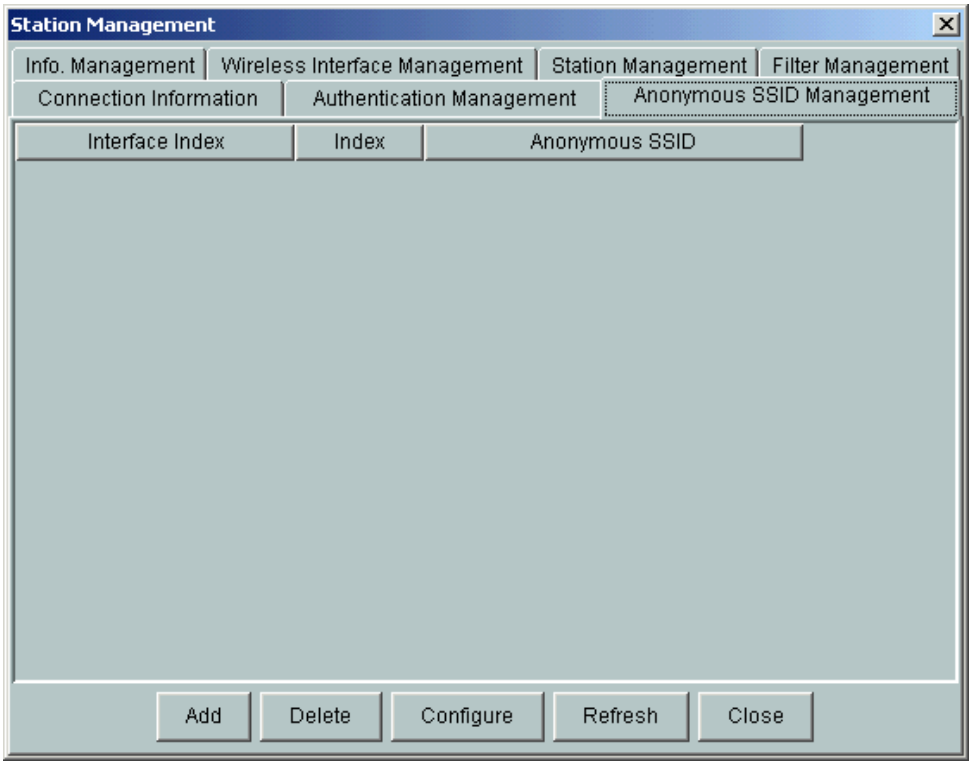


Figure 11-11 Anonymous SSID Management

Click <Add> in the [Anonymous SSID Management] dialog box, then the [Add Anonymous SSID] dialog box appears.

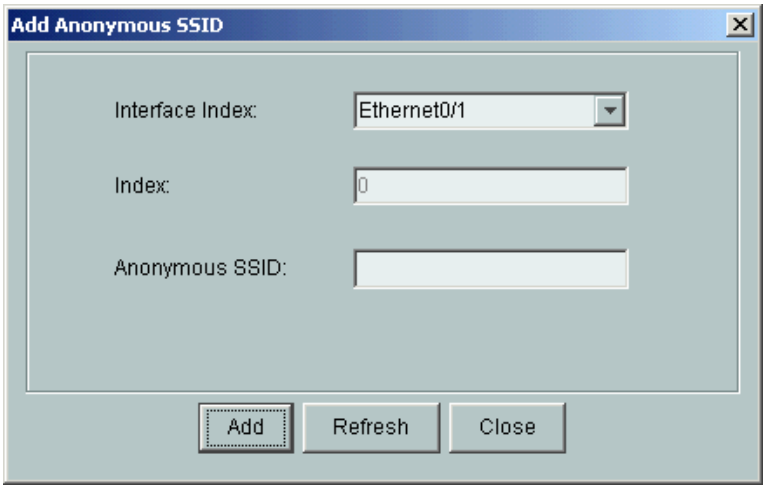


Figure 11-12 Add Anonymous SSID

11.4 Physical Layer Management

Start Quidview Device Manager, select the [Device/Open…] from the menu or click on the toolbar to display the panel view of your WLAN device and click <Physical Layer Management> in the function navigation window. Then the [Physical Layer Management] dialog box appears.

11.4.1 Antenna Management

In the [Physical Layer Management] dialog box, select the [Antenna Management] tab. Then the [Antenna Management] interface appears, as shown in Figure 11-13.

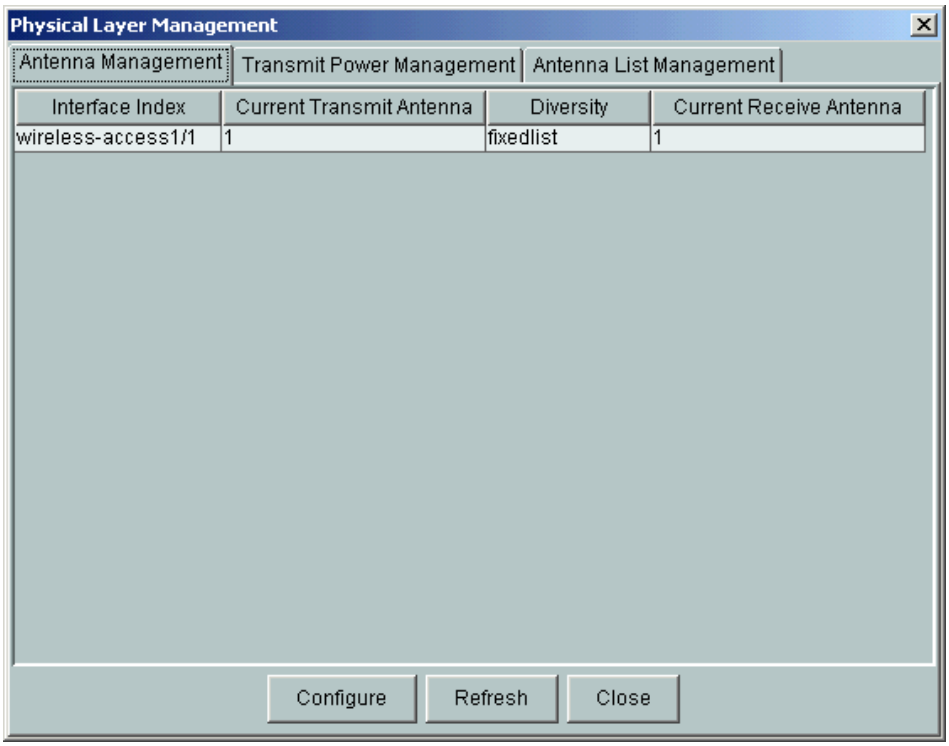


Figure 11-13 Antenna Management

The dialog box displays the current transmit antenna, diversity and current receive antenna of your AP device ports.

Select the interface index that you want to modify and click <Configure…>, then the [Modify Antenna Info] dialog box appears.

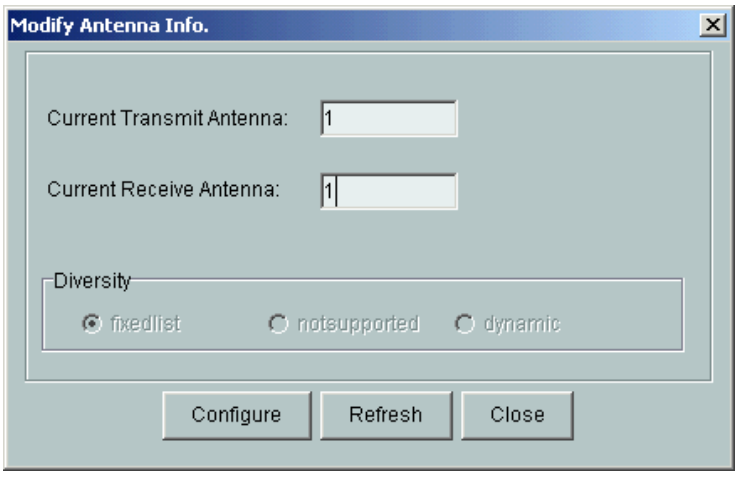


Figure 11-14 Modify Antenna Info

The values of current transmit antenna and current receive antenna can be 0,1,2 or 3, which respectively indicates that the receive antenna is antenna 1, antenna 2, total diversity or part diversity.

There are three options for diversity: fixed list, not supported and dynamic.

11.4.2 Transmit Power Management

In the [Physical Layer Management] dialog box, select the Transmit Power Management tab. Then the [Transmit Power Management] interface appears, as shown in the following figure.

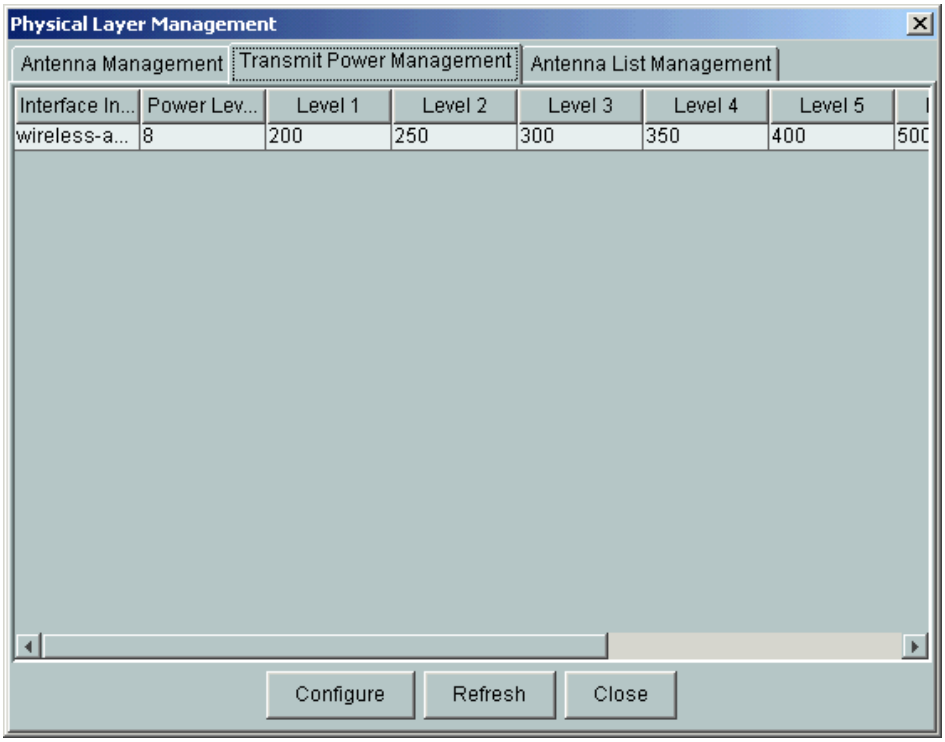


Figure 11-15 Transmit Power Management

This dialog box displays the transmit power of your AP device ports that ranges from level 1 to level 8.

Select the interface index that you want to modify and click <Configure…>, then the [Modify Transmit Power Info] dialog box appears. Select appropriate value in the drop-down list box Current Transmit Power Level to reconfigure the level for the port.

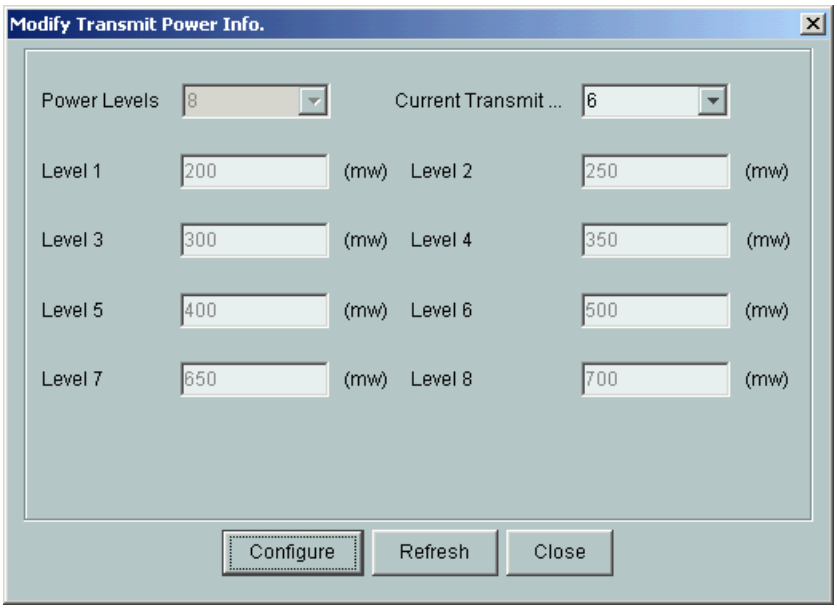


Figure 11-16 Modify Transmit Power Info

11.4.3 Antenna List Management

In the [Physical Layer Management] dialog box, select the [Antenna List Management] tab, then the [Antenna List Management] interface appears.

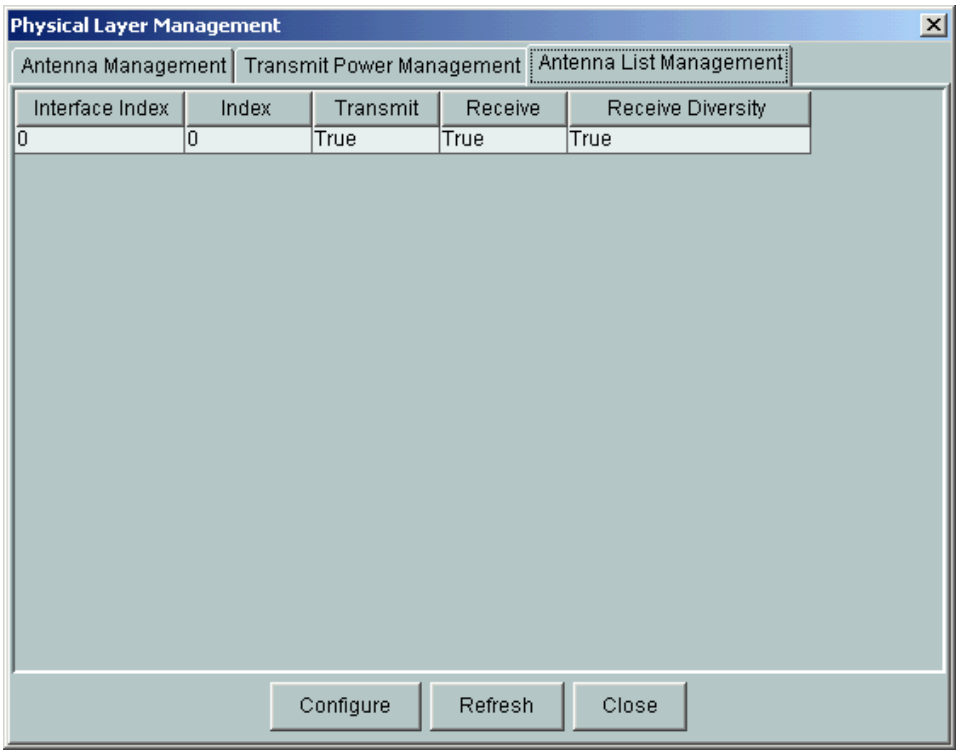


Figure 11-17 Antenna List Management

This dialog box displays the information including Transmit, Receive and Receive Diversity.

Select the interface index that you want to modify and click <Configure…>, then the [Modify Antenna list Info.] dialog box appears.

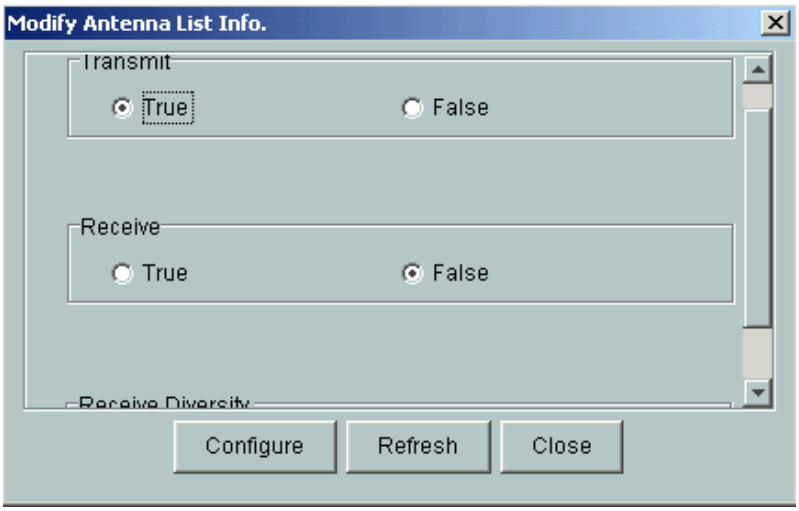


Figure 11-18 Modify Antenna list Info

11.5 Encryption Management

AP supports 64-bit, 128-bit and 256-bit WEP encryption.

Start Quidview Device Manager, select [Device/Open…] from the menu or click on the toolbar to display the panel view of your WLAN device. In the function navigation window, click <Encryption Management>. Then the [Encryption Management] dialog box appears.

11.5.1 Encryption Table Management

In the [Encryption Management] dialog box, select the [Encryption Table Management] tab, then the [Encryption Table Management] interface appears.

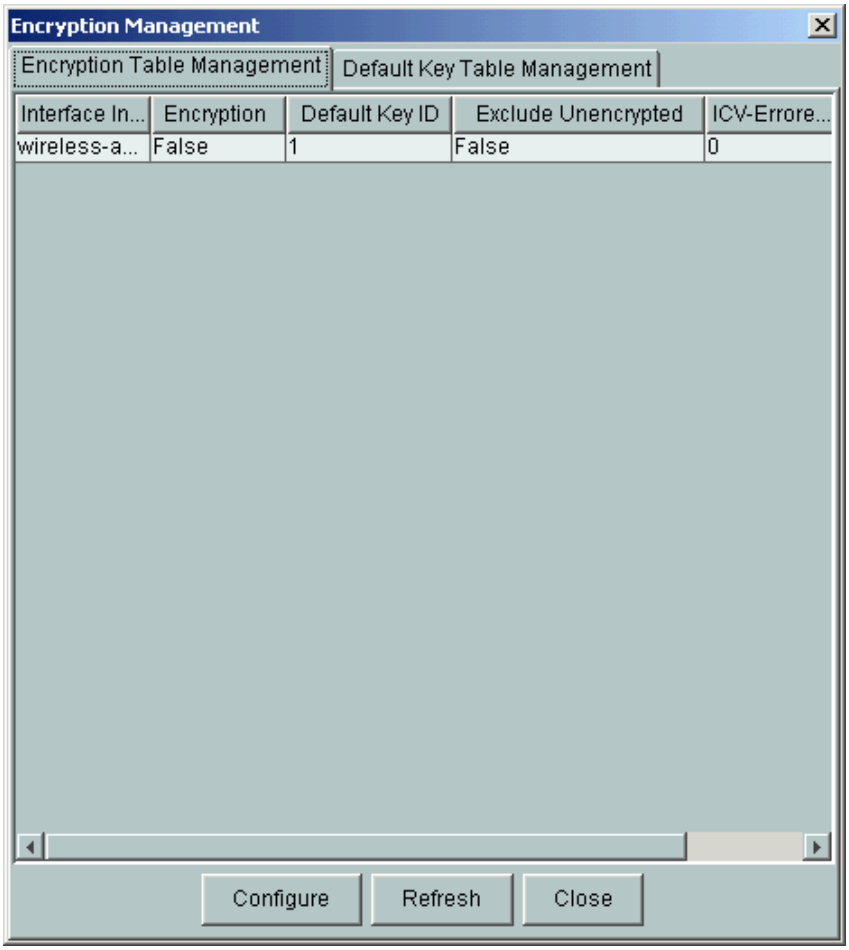


Figure 11-19 Encryption Table Management

This dialog box displays the following encryption table information about each port on the AP device: Encryption, Default Key ID, Exclude Unencrypted, ICV Error Frames and Excluded Unencrypted Frames.

Select the interface index that you want to modify and click <Configure…>, then the [Modify Encryption Info.] dialog box appears as shown in the following figure. You can reconfigure such encryption attributes of the port as Encryption and Exclude Unencrypted, and select one Default Key ID from the drop-down list box. Refer to the next section for more information about the default key ID management.

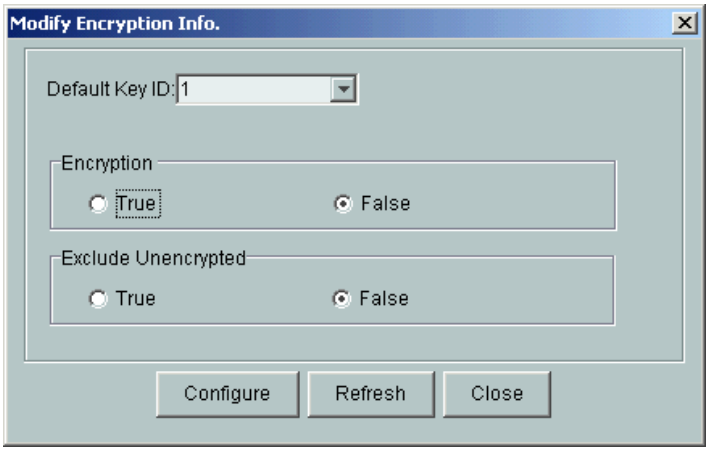


Figure 11-20 Modify Encryption Info

11.5.2 Default Key Table Management

In the [Encryption Management] dialog box, select the [Default Key Table Management] tab, then the [Default Key Table Management] interface appears, as shown in the figure below.

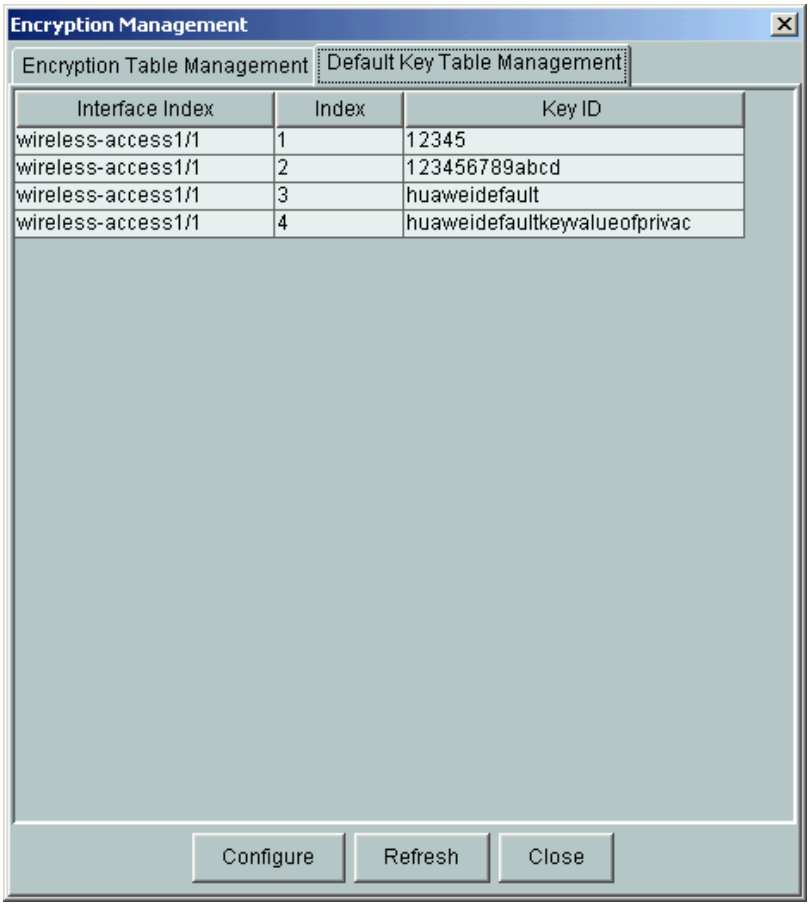


Figure 11-21 Default Key Table Management

Select the interface index that you want to modify and click <Configure…> to configure the default key.

11.6 Performance Statistics

Start Quidview Device Manager, select [Device/Open…] from the menu or click on the toolbar to display the panel view of your WLAN device, click <Performance Statistics> in the function navigation window and the [Performance Statistics] dialog box appears as shown in the figure below.

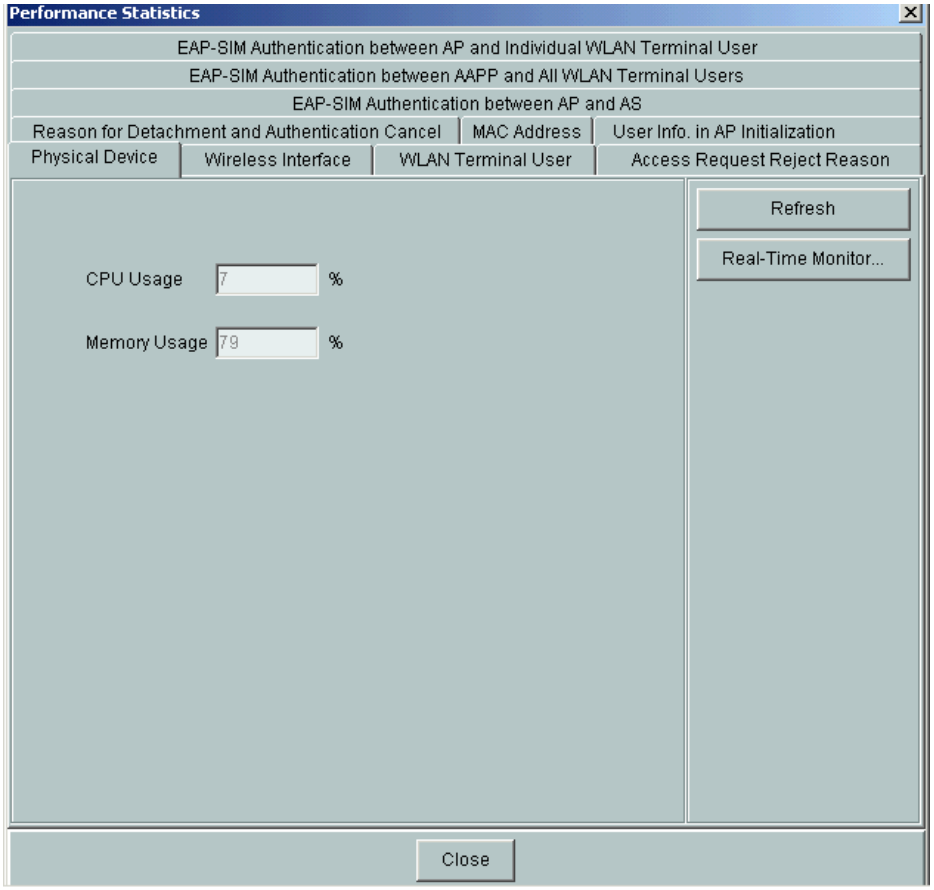


Figure 11-22 Performance Statistics

Physical Devices

In the [Performance Statistics] dialog box, select the [Physical Devices] tab, then the [Physical Devices] interface appears, which displays the CPU Usage and Memory Usage of your AP device.

Click <Real-Time Monitor…> to show real-time statistics of CPU Usage and Memory Usage.

11.6.1 Wireless Interface

In the [Performance Statistics] dialog box, select the Wireless Interface tab. Then the "Wireless Interface" interface appears, which displays Port Description, Frames Discarded at Wireless Interface, Total Frames Failed to Be Transmitted, Total Frames with CRC Error at MAC Layer, Frames with SSIDs Other Than the Pre-Defined, AP Authentication Counts at MAC layer, AP Authentication Failures at MAC Layer.

Click <Real-Time Monitor…> to display real-time statistics of the above items.

11.6.2 WLAN Terminal User

In the [Performance Statistics] dialog box, select the WLAN Terminal User tab, then the "WLAN Terminal User" interface appears, which displays Port Description, Associate Attempts, Successful Associates, Current Associated Users, Reassociate Attempts, Successful Reassociates, and Current Reassociated Users.

Click <Real-Time Monitor…> to display real-time statistics of the above items.

11.6.3 Access Request Reject Reason

In the [Performance Statistics] dialog box, select the [Access Request Reject Reason] tab. Then the [Access Request Reject Reason] interface appears, which displays port descriptions, code 1, code 10, code 11, code 12, code 13, code 14, code 15, code 16, code 17 and code 18.

Click an item in the [Access Request Reject Reason] interface to show details on reject reasons.

Click <Real-Time Monitor…> to display real-time statistics of the above items.

11.6.4 Reason for Detachment and Authentication Cancel

In the [Performance Statistics] dialog box, select the [Reason for Detachment and Authentication Cancel] tab. Then the [Reason for Detachment and Authentication Cancel] interface appears, which displays port description, code 1, code 10, code 11, code 12, code 13, code 14, code 15, code 16 and code 17.

Click an item in the [Reason for Detachment and Authentication Cancel] interface to show details on reasons of failures.

Click <Real-Time Monitor…> to display real-time statistics of the above items.

11.6.5 MAC Address

In the [Performance Statistics] dialog box, select the MAC Address tab. Then the [MAC Address] interface appears, which displays Total Current MAC Addresses.

11.6.6 User Info. In AP Initialization

In the [Performance Statistics] dialog box, select the User Info. In AP Initialization tab, then the [User Info. In AP Initialization] interface appears. It displays Total Get-Online Times, Current Online Users, Normal Get-Offline Times, and Abnormal Get-Offline Times.

Click <Real-Time Monitor…> to display real-time statistics of the above items.

11.6.7 EAP-SIM Authentication between AP and AS

In the [Performance Statistics] dialog box, select the EAP-SIM Authentication between AP and AS tab, then the [EAP-SIM Authentication between AP and AS] interface appears. It displays AP UNDER EAP-SIM Authentication EAP-SIM, total Requests towards AS Server (authentication) and Total Requests towards AS Server (account).

Click <Real-Time Monitor…> to display real-time statistics of the above items.

11.6.8 EAP-SIM Authentication between AAPP and All WLAN Terminal Users

In the [Performance Statistics] dialog box, select the [EAP-SIM Authentication between AAPP and All WLAN Terminal Users] tab, then the [EAP-SIM Authentication between AAPP and All WLAN Terminal Users] interface appears. It displays Total Transmitted EAP-Request/Identify Packets, Total Received EAP-Response/Identify Packets, Total Transmitted EAP-Request/SIM/Challenge Packets, Retransmitted EAP-Request/ SIM/Challenge Packets, Received EAP-Response/SIM/Challenge Packets, Total Received EAPoL-Start Packets, and Total Transmitted EAP-Success Packets.

Click <Real-Time Monitor…> to display real-time statistics of the above items.

11.6.9 EAP-SIM Authentication between AP and Individual WLAN Terminal User

In the [Performance Statistics] dialog box, select the [EAP-SIM Authentication between AP and Individual WLAN Terminal User] tab, then the [EAP-SIM Authentication between AP and Individual WLAN Terminal User] interface appears. It displays Total Received EAPoL-Start Packets from User Terminal and Total Transmitted EAPoL-Start Packets to User Terminal.

Click <Real-Time Monitor…> to display real-time statistics of the above items.

Chapter 12 SMON Management

SMON (Switched Networks Monitoring) is an application of RMON to switched networks. It includes the following contents:

- SMON data source query
- VLAN statistics management
- VLAN priority statistics management

At present, SMON is supported by S5516 Switch only.

12.1 SMON Data Source Management

Start Quidview Device Manager and select [Device/Open Device…] or click on the toolbar to open the panel view of an Ethernet switch. In the function window, click "+" corresponding to the [Performance monitor] node and double-click on the [SMON] leaf node to open the [SMON] dialog box, as shown in Figure 12-1:

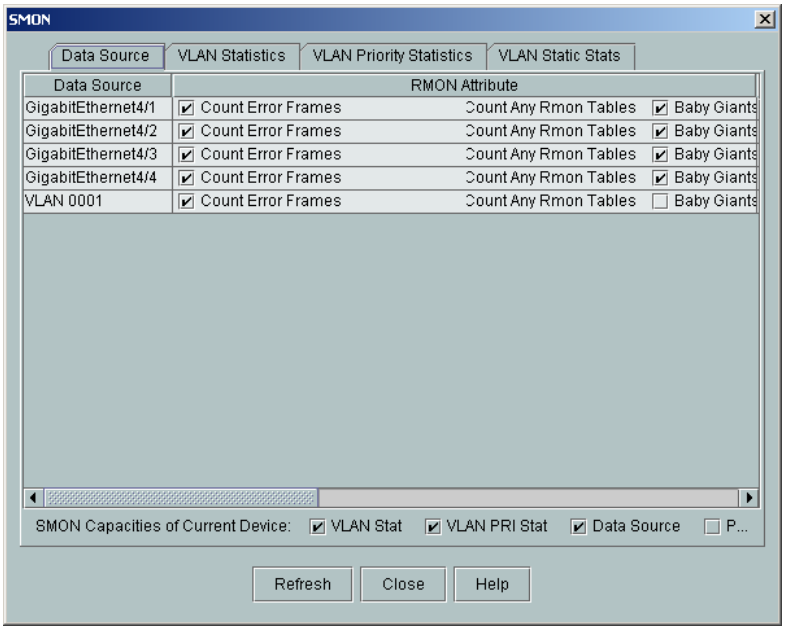


Figure 12-1 SMON data source

SMON extends the concept of data source in RMON and includes the following three types of data sources:

- Interface-oriented data source: the traditional RMON data source that is the value of interface index
- VLAN-oriented data source: the value of VLAN ID in the specified range
- Entity-oriented data source: a physical entity such as a board or a switch

The [Data Source] page shows the attributes of the configured SMON data sources in the system, as listed in Table 12-1:

Table 12-1 SMON data source information

Field	Meaning
Data source	Name of data source that can be an interface index, VLAN ID or entity name
SMON attributes	SMON support capacity provided by current data source, including: 1: Count Error Frames 2: Count All Good Frame 3: Count Applicable Data Sources 4: Baby Giants Count As Good
Copy attributes	Include: Copy source port Copy dest port Copy src txTraffic Copy src RxTraffic Copy dest drop events Copy error frames Copy unaltered frames Copy all good frames
Index	Index of data source
SMON capacity of current device	Include: VLAN stat VLAN pri stat Data source Port copy

12.2 VLAN Statistics Management

The VLAN statistics of SMON provides the information about VLAN load and overall healthy conditions. By configuring VLAN statistics table on the NM station, you can implement monitoring on different VLAN virtual interfaces. Polling the table periodically, you can get VLAN load and healthy condition information

1) Add a VLAN statistic item

In Figure 12-1, click the [VLAN Statistics] tab to switch to the [VLAN Statistics] page, as shown in Figure 12-2:

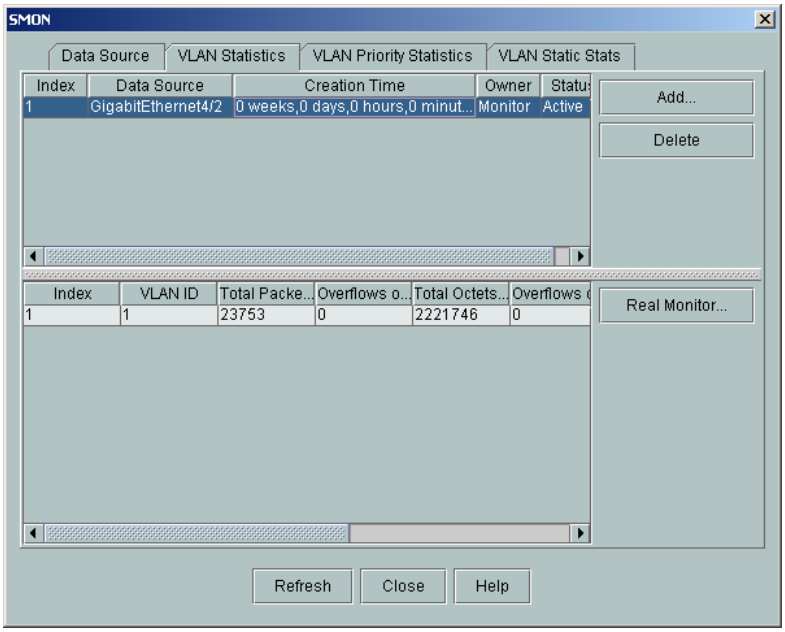


Figure 12-2 Configuring and browsing VLAN statistics

This interface is broken into two panes. The upper pane shows all the predefined VLAN statistic items on the device, and the meaning of various fields is described in Table 12-2. The functional buttons on the right provide configuration and browsing for VLAN statistics. The lower pane shows all the sub-items contained in the selected VLAN statistic items, and the meaning of various fields is described in Table 12-3. The functional button on the right provides real-time monitoring function for one or several VLAN statistic items.

Table 12-2 Contents of a VLAN statistic item

Content	Description
Index	Index of a VLAN statistic item
Data source	Name of data source
Creation time	Creation time of the VLAN statistic item
Owner	Owner of the VLAN statistic item
Status	Include Active, noReady and Inactive

Table 12-3 Contents of a VLAN statistic sub-item

Content	Description
Index	Index of the VLAN statistic sub-item
VLAN ID	VLAN ID corresponding to the sub-item
Total packets (32 bits)	Total

Content	Description
Overflows of total packets	
Total octets (32 bits)	
Overflows of total octets	
Unicast packets(32 bits)	
Overflows of unicast packets	
Unicast octets (32 bits)	
Overflows of unicast octets	

Click <Add…> to open the [Add VLAN Statistics Information] dialog box, as shown in Figure 12-3:

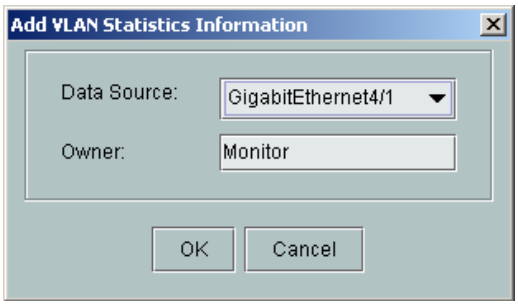


Figure 12-3 Adding a VLAN statistic item

The information required by the interface is listed in Table 12-4:

Table 12-4 Contents required by adding a VLAN statistic item

Content	Description
Data source	You must specify a data source for a VLAN statistic item from the drop-down list.
Owner	Creator of the collection task. By default, it is "Monitor".

2) Delete a VLAN statistic item

In Figure 12-2, select one or more VLAN statistic items and click <Delete> to open the confirmation dialog box, where click <OK> to delete the selected VLAN statistic items.

3) Monitor a VLAN statistic item on a real-time basis

In Figure 12-2, select one or more VLAN statistic items from the upper list and data item(s) to be monitored from the lower list, and then click <Real Monitor…> to open the [SMON Traffic Monitoring] dialog box, as shown in the following figure:

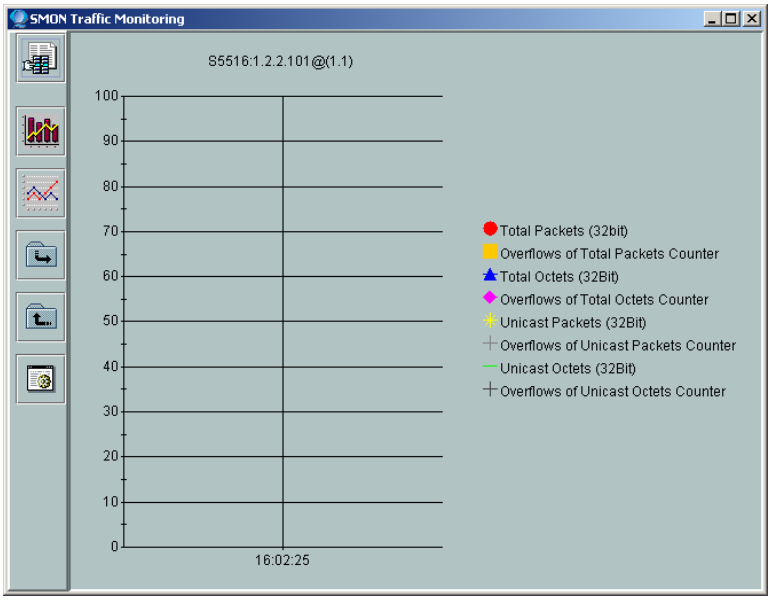


Figure 12-4 Real-time monitoring of VLAN statistic items

Click in Figure 12-4 to open the [Select Statistics Items] dialog box, as shown in the following figure:

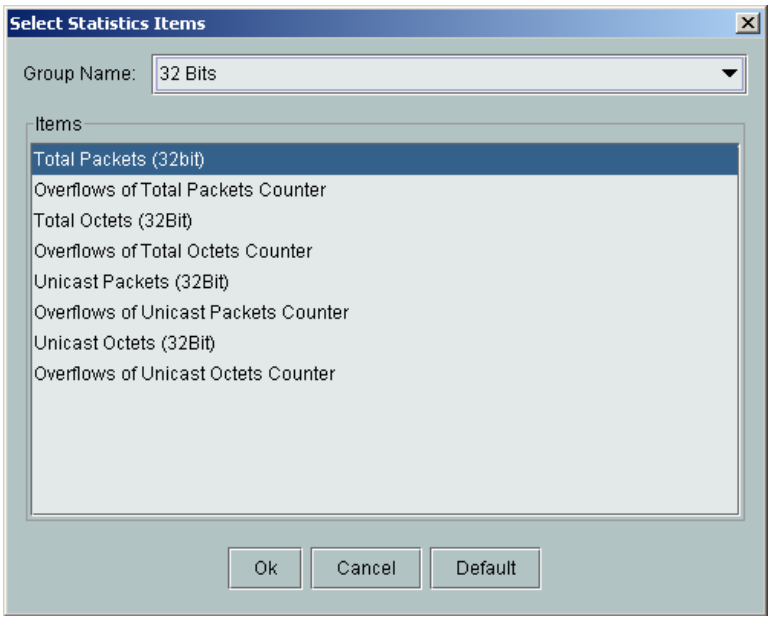


Figure 12-5 Selecting VLANT statistic items

Select the monitoring items and click <OK> to perform real-time monitoring on the specified data source addressing the selected items.

12.3 VLAN Priority Statistics Management

The VLAN priority statistics of SMON provides the information about priority load and overall healthy conditions. By configuring VLAN priority statistics table on the NM station, you can monitor different VLAN priorities. Polling the information in the table periodically, you can get the load and overall healthy condition information of the various VLANs.

1) Add a VLAN priority statistic item

In Figure 12-1, click the [VLAN Priority Statistics] tab to switch to the configuration and browsing page for VLAN priority statistics, as shown in the following figure:

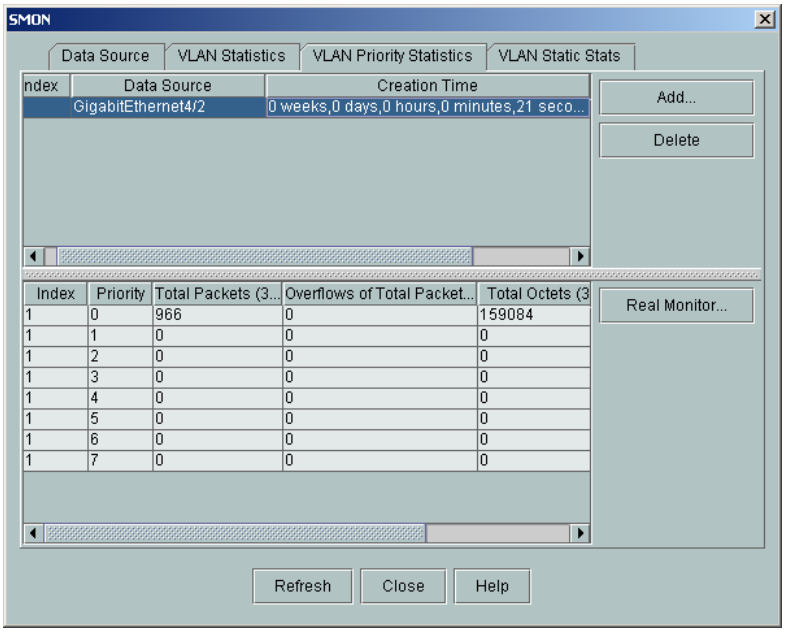


Figure 12-6 Configuring and browsing VLAN priority statistics

This interface is broken into two panes. The upper pane shows all the predefined VLAN priority statistic items on the device, and the meaning of various fields is described in Table 12-5. The functional buttons on the right provide configuration and browsing for VLAN priority statistics. The lower pane shows all the sub-items contained in the selected VLAN priority statistic item, and the meaning of various fields is described in Table 12-6. The functional button on the right provides real-time monitoring function for one or several VLAN priority statistic items.

Table 12-5 Contents of a VLAN priority statistic item

Content	Description
Index	Index of a VLAN statistic item
Data source	Name of data source
Creation time	Creation time of the VLAN statistic item

Content	Description
Owner	Owner of the VLAN statistic item
Status	Include Active, noReady and Inactive

Table 12-6 Contents of a VLAN priority statistic sub-item

Content	Description
Index	Index of the VLAN statistic sub-item
Priority	Priority of the sub-item
Total packets (32 bits)	
Overflows of total packets	
Total octets (32 bits)	
Overflows of total octets	

Click <Add…> in Figure 12-6 to open the [Add VLAN Priority Statistics Information] dialog box, as shown in the following figure:

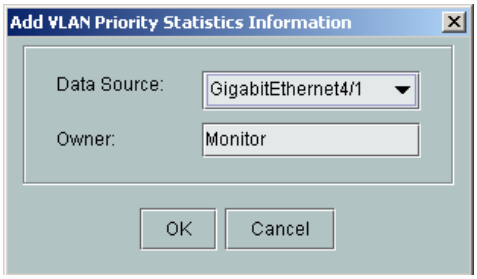


Figure 12-7 Adding a VLAN priority statistic item

The information required by the interface is listed in Table 12-7.

Table 12-7 Contents required by adding a VLAN priority statistic item

Content	Description
Data source	You must specify a data source for a VLAN priority statistic item from the drop-down list.
Owner	Creator of the collection task. By default, it is "Monitor".

2) Delete a VLAN priority statistic item

In Figure 12-6, select one or more VLAN priority statistic items and click <Delete> to open a confirmation dialog box, where click <OK> to delete the selected items.

3) Monitor a VLAN priority statistic item on a real-time basis

In Figure 12-6, select one or more VLAN priority statistic items from the upper list and data item(s) to be monitored from the lower list, and then click <Real Monitor…> to open the [SMON Traffic Monitoring] dialog box, as shown in the following figure:

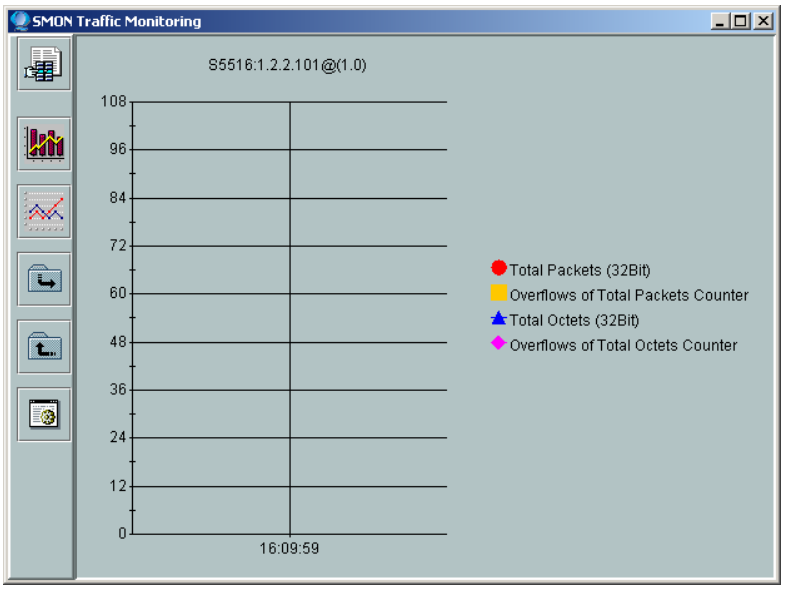


Figure 12-8 Real-time monitoring of VLAN priority statistic items

Click in above interface to open the [Select Statistics Items] dialog box, as shown in the following figure:

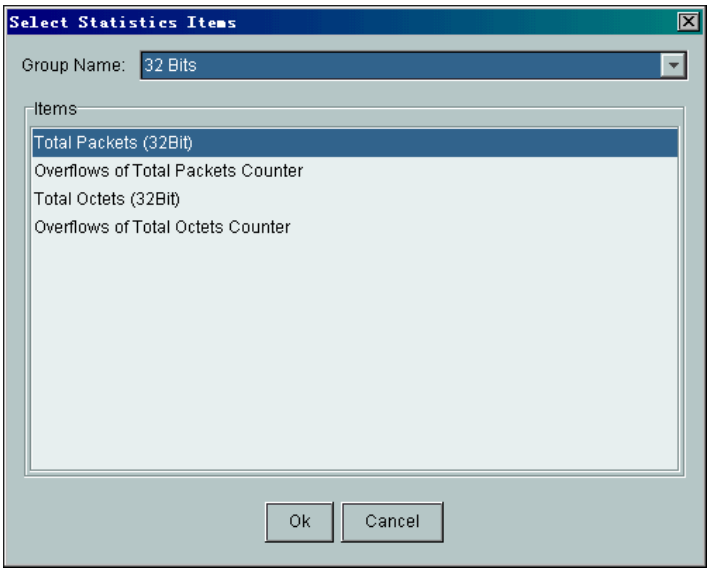


Figure 12-9 Selecting VLAN priority statistic items

Select the monitoring items and click <OK> to perform real-time monitoring on the specified data source addressing the selected items.

12.4 VLAN Static Statistics Management

The function allows you to query and configure VLAN static statistic status.

Click the [VLAN Static Statistic Status] tab to switch to the browsing and configuration page for VLAN static statistics. Select one or more lines of data to be configured, and then click <Config…>. In the popup dialog box, input proper data, and then click <OK> to complete the modification.

Chapter 13 RPR Management

Resilient Packet Ring (RPR) integrates the intelligence of IP, economy of Ethernet as well as the broad width and reliability of fiber-optic ring network to provide a perfect networking solution for broad band IP Metropolitan Area Network (MAN) carriers.

The chapter mainly introduces the RPR management function of Device Manager for S8500 (a kind of high-end switch). The RPR interface management provided by Device Manager for high-end routers (such as NE80) is different from the RPR management introduced here; for detailed description on the RPR interface management, refer to the related sections in Quidview Device Manager User Manual Volume I.

13.1 Logical and Physical Interfaces of RPR

On the S8500 switch, two RPR physical interfaces comprise a logical one. Figure 13-1 illustrates the RPR physical interfaces on the S8500 device panel and the physical interfaces serve as the sub interfaces of the logical one, for example, if the logical interface is RprPos3/1/1, the physical interfaces are RprPos3/1/1.1 and RprPos3/1/1.2.

Figure 13-1 Physical interfaces of RPR

Caution:

- If there are only two physical interfaces on the S8500 switch, the logical interface will not change whichever the physical interface the user selects, because the two physical interfaces belong to the same logical interface. As shown in Figure 13-1, whether you select the physical interface RprPos3/1/1.1 or RprPos3/1/1.2, the displayed logical interface on the function interface opened in Device Manager is always RprPos3/1/1.
- Currently, RPR can be classified into 2.5G RPR and 10G RPR. There are two types of physical interfaces for 10G RPR: RprPos (10G) and Rpr10GE, and one type for 2.5G RPR: RprPos.

13.2 RPR Interface Management

RPR interface management is used to configure and view RPR related parameters.

Double-click the [RPR Management/RPR Interface Management] node on the function tree and the system pops up the [RPR Interface Management] window, as shown in Figure 13-2.

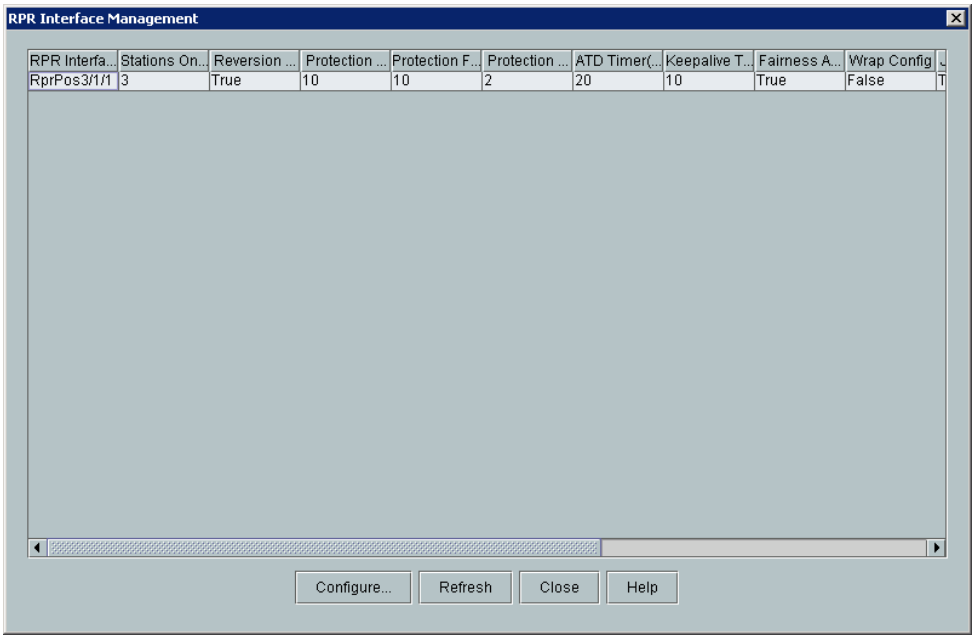


Figure 13-2 RPR Interface Management

Select one or more interfaces, click <Configure…> and then the system pops up the [RPR Interface Configuration] dialogue box, as shown in Figure 13-3.

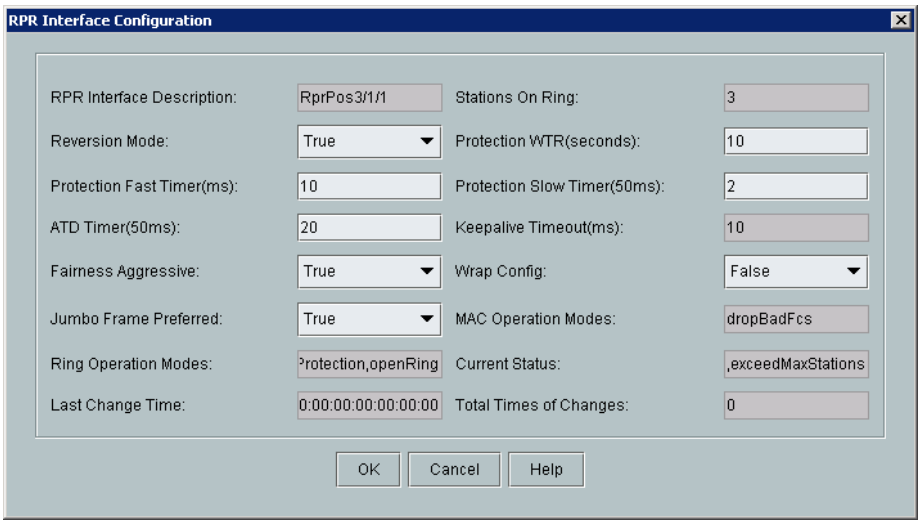


Figure 13-3 RPR Interface Configuration

You can modify the parameters and click <OK> to deploy the new configuration to devices. The description on the parameters in the [RPR Interface Configuration] dialogue box is shown in Table 13-1.

Table 13-1 Description on the parameters of RPR interface configuration

Name	Description
RPR Interface Description	Description on the logical interface.
Stations On Ring	The number of stations contained on the ring where the current RPR interface resides. If the operation status of the interface is “down”, the value is 1.
Reversion Mode	The reversion mode of MAC. “False” is for denied and “True” is for permitted. If “True” is selected, the reversion station will be restored to the idle state when WTR interval expires.
Protection WTR (seconds)	The buffer time to remove the auto protection, in second. The mechanism can emulate the jitter of protection alternation and ranges from 0 to 1440 seconds.
Protection Fast Timer (ms)	The clock quickly sent by the TP frame, ranges from 1 to 20 milliseconds.
Protection Slow Timer (50 ms)	The clock slowly sent by the TP frame. It is used for protocol protection and topology, ranges from 1 to 200 milliseconds.
ATD Timer (50 ms)	Interval of the Attribute Discover (ATD) frame transmission and the value is the result of the value set by the user multiplying 50 milliseconds. For example, if the value set by the user is 20, the frame transmission interval is 20 times of 50 milliseconds, namely one second. The range of the interval is from 1 to 200 milliseconds, in 50 milliseconds.
Keepalive Timeout (ms)	Timing interval of Keepalive.
Fairness Aggressive	The sign indicating whether the fairness algorithm adopts the aggressive mode.
Wrap Config	Wrap mode, can be Wraping or Steering.
Jumbo Frame Preferred	Whether jumbo frame is supported.
MAC Operation Modes	The detailed information of MAC operation modes. “dropbadFcs” means that the frames with bad FCS will be discarded; and “strictorder” refers that MAC operates in strict order mode.

Name	Description
Ring Operation Modes	The summary of the ring operational modes collected through the topology discovery protocol. Only if all stations on the ring are configured to support jumbo frames, the value contains the jumbo frames supported information. Only if all stations on the ring are configured to Wrap mode, the value contains the Wrap mode information. If the ring doesn't complete a full loop, the value contains the openRing information.
Current Status	Current status of the RPR interface.
Last Change Time	Last change time.
Total Times of Changes	Total times of changes.

13.3 Statistic Data Management

Statistic data management is responsible for configuring the statistic counter, namely clearing the buffer data of monitor saved on devices.

Double-click the [RPR Management/Statistic Data Management] node on the function tree, and the system pops up the [Statistic Data Management] dialogue box, as shown in Figure 13-4.

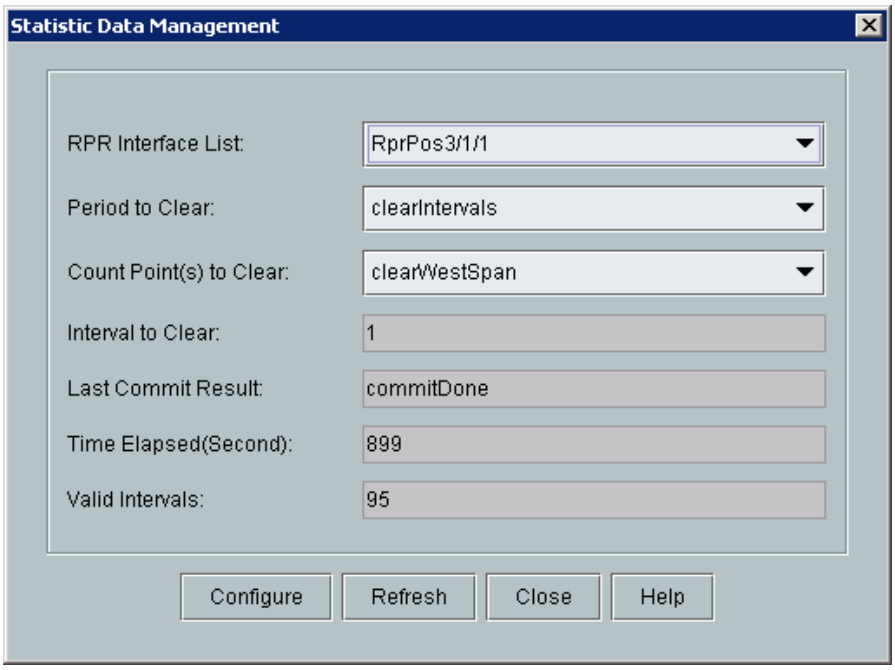


Figure 13-4 Statistic Data Management

You can modify the parameters and click <Configure…> to deploy the new configuration. The description on the parameters in the [Statistic Data Management] dialogue box is shown in Table 13-2.

Table 13-2 Description on the parameters of statistic data management

Name	Description
RPR Interface List	List of logical interfaces, all the RPR interfaces on the current station are listed.
Period to Clear	The periods to be cleared are as follows: • Idle: no clearing is performed; • clearAllIntervals: clears all the data of the buffer counter on the RPR interface; • clearCurrent: clears the data of buffer counter used to support the data monitoring for the last 15 minutes; • clearIntervals: clears the all the data of buffer counter except for the ones used in the last 15 minutes; • clearSpecificInterval: specifies the value of the parameter ”Interval to Clear”.
Count Point(s) to Clear	The count points to be cleared are as follows: • clearWestSpan&EastSpan&Client: clears the buffer counter data of the west and east spans and the client; • clearWestSpan: clears the buffer counter data of the west span; • clearEastSpan: clears the buffer counter data of the east span; • clearClient: clears the buffer counter data of the client.
Interval to Clear	Intervals to be cleared. It is only valid when the parameter “clearSpecificInterval” is selected in the [Period to Clear] field, and its value ranges from 1 to 96.
Last Commit Result	Last commit result, and the corresponding commit information is displayed according to the clearing result.
Time Elapsed (Second)	Elapsed time of the data record for the current interval.
Valid Intervals	The number of intervals of the last 15 minutes.

13.4 Protection Parameters Configuration

Protection parameters configuration enables you to configure and query the protection parameter information of the specified Span.

Double-click the [RPR Management/Protection Parameters Configuration] node on the function tree, and the system pops up the [Protection Parameters Configuration] dialogue box, as shown in Figure 13-5.

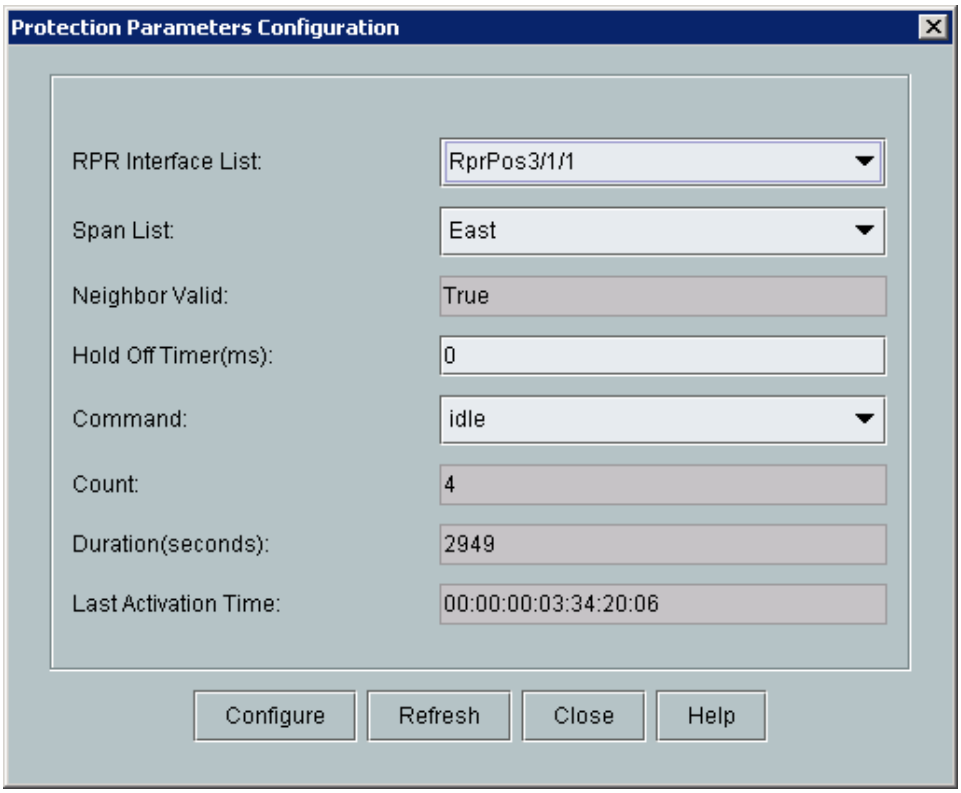


Figure 13-5 Protection Parameters Configuration of Span

You can modify the parameters and click <Configure…> to deploy the new configuration. The description on the parameters in the [Protection Parameters Configuration] dialogue box is shown in Table 13-3.

Table 13-3 Description on the parameters of protection parameters configuration

Name	Description
RPR Interface List	List of logical interfaces, all the RPR interfaces on the current station are listed.
Span List	Lists the Span of the logical interface.
Neighbor Valid	Indicates whether the address neighboring the Span is valid.
Hold Off Timer (ms)	The threshold used by RPR to activate the protection mechanism at the bottom layer. The cable plug-off and signal attenuation are not counted as Failure. The value ranges from 0 to 500 milliseconds.

Name	Description
Command	Used to read and change the protection status. Returns the last submitted protection command (except that it is preempted) when reading the protection status. If no command is configured on the Span since initialization, “idle” is returned. The commands allow to be configured include: idle, manualSwitch, and forcedSwitch. Whether the settings are configured successfully depends on the current priority of the protection mode on the device. If the current protection mode is ”idle” and the link is normal, “manualSwitch” and “forcedSwitch” can be configured. If the current protection mode is ”idle” and the link is abnormal, only the “forcedSwitch” can be configured. If the current protection mode is “manualSwitch”, “forcedSwitch” and ”idle” can be configured. ”idle” means clearing all the manual and forced protection modes,
Count	Activation counts of the protection mode.
Duration (seconds)	Duration of the Span in the protection mode.
Last Activation Time	The last activation time of the protection mode.

13.5 Fairness Management

Fairness management dynamically regulates network traffic (including bursty large data traffic) to avoid network congestion and ensure network availability.

Fairness Management provides configuration and query functions on the specified fairness parameters.

Double-click the [RPR Management/Fairness Management] node on the function tree, and the systems pops up the [Fairness Management] dialogue box, as shown in Figure 13-6.

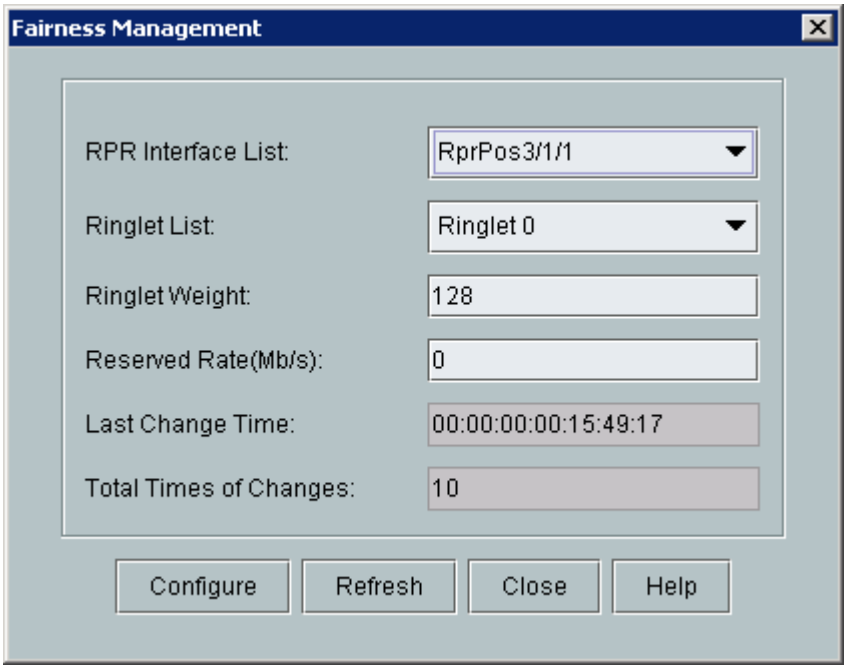


Figure 13-6 Fairness Management

You can modify the parameters and click <Configure…> to deploy the new configuration. The description on the parameters in the [Fairness Management] dialogue box is shown in Table 13-4.

Table 13-4 Description on the parameters of fairness management

Name	Description
RPR Interface List	List of logical interfaces, all the RPR interfaces on the current station are listed.
Ringlet Weight	The weighted value of the station in the current ringlet, ranges from 1 to 128. The ringlet weight enables some stations to possess more bandwidth without violating fairness rules.
Reserved Rate (Mb/s)	The reserved rate of the current station for the service A0. it can be zero or positive integer, in Mb/s.
Last Change Time	Last change time with the displayed format being as: year:month:day:hour:minute:second:millisecond.
Total Times of Changes	Total times of changes of the “Last Change Time”.

13.6 OAM Management

OAM management is used to check the connectivity between the stations on the ring. You can modify the OAM parameters of the specified RPR interface and perform OAM operations to check the connectivity between the stations on the ring.

Double-click the [RPR Management/OAM Management] node on the function tree, and the system pops up the [OAM Management] dialogue box, as shown in Figure 13-7.

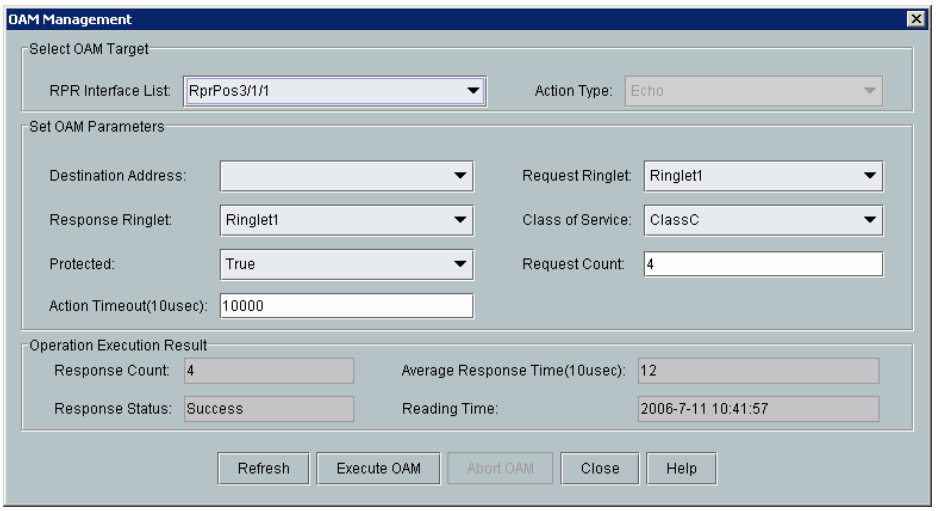


Figure 13-7 OAM Management

You can modify the parameters and click <Execute OAM> to deploy the new configuration and execute the specified OAM operation. The description on the parameters in the [OAM Management] dialogue box is shown in Table 13-5.

Table 13-5 Description on the parameters of OAM management

Name	Description
RPR Interface List	List of logical interfaces, all the RPR interfaces on the current station are listed.
Action Type	There are two types: Flush and Echo. Currently, only Echo is available.
Destination Address	Destination MAC address of the 48-bit OAM session.
Request Ringlet	Indicates from which ringlet the OAM request is sent.
Response Ringlet	Indicates on which ringlet the OAM response is received.
Class of Service	Indicates the service class information in OAM session frames. The available types are: Class A, Class B and Class C.
Protected	Indicates whether OAM actions are protected.
Request Count	The number of OAM requests to be sent, ranges from 0 to 65535.
Action Timeout (10usec)	Indicates the timeout of OAM actions, in 10 milliseconds, ranges from 1 to 10000.
Response Count	The number of received OAM responses.

Name	Description
Average Response Time (10usec)	Indicates the average response time for receiving OAM requests, in 10 milliseconds.
Response Status	Indicates the status of OAM actions. If more than 90% requests are returned earlier than the timeout, the response status is “success”.

13.7 Span Browsing

Span Browsing enables you to view the west and east Span information of the specified RPR interface.

Double-click the [RPR Management/Span Browsing] node on the function tree, and the system pops up the [Span Browsing] window. The description on the parameters in the [Span Browsing] window is shown in Table 13-6.

Table 13-6 Description on the parameters of Span browsing

Name	Description
RPR Interface List	List of logical interfaces, all the RPR interfaces on the current station are listed.
Lower Layer Interface	Description on the physical interfaces of the Span.
Current Status	The current status of the Span.
Total Ringlet Reserved Rate	The bandwidth on the ringlet reserved for the service A0.
Last Change Time	Last change time of any one of the five parameters, that is, “Current Status” of Span and the four parameters specified in protection parameter configuration: “Neighbor Valid”, “Hold Off Timer (ms)”, “Command” and “Count”.
Total Times of Changes	Total times of changes of the “Last Change Time”.

13.8 TOPO Ring Browsing

TOPO ring browsing is used to browse the topology ring information on the RPR interface.

Double-click the [RPR Management/TOPO Ring Browsing] node on the function tree, and the system pops up the [TOPO Ring Browsing] window. The description on the parameters in the [TOPO Ring Browsing] window is shown in Table 13-7.

Table 13-7 Description on the parameters of TOPO ring browsing

Name	Description
RPR Interface List	List of logical interfaces, all the RPR interfaces on the current station are listed.
MAC Address	Unique MAC address of the station on a ring.
Station Interface Index	RPR interface index of the station.
Station Name	Name of the station.
IP Address Type	Types of IP address, IPV4 or IPV6.
IP Address	IP address of the station.
Status	Status of the station including the accessibility of station through ringlet 0 and ringlet 1, wrap active on the station spans, events of reception frames with bad FCS and so on.
Capability	Indicates the capabilities that the MAC supports.
Ringlet 0 Hops	The number of hops to this station through ringlet 0. The self station is indicated with zero hops.
Ringlet 0 Reserved Rate	The reserved rate of the station on ringlet 0.
Ringlet 1 Hops	The number of hops to this station through ringlet 1. The self station is indicated with zero hops.
Ringlet 1 Reserved Rate	The reserved rate of the station on ringlet 1.
West Protection Status	The current protection status of the west span.
West Weight	The weight of the station on the west span.
East Protection Status	The current protection status of the east span.
East Weight	The weight of the station on the east span.
MAC Address 1	The 48-bit first secondary MAC address of the station. Default and unused value is FF:FF:FF:FF:FF:FF.
MAC Address 2	The 48-bit second secondary MAC address of the station. Default and unused value is FF:FF:FF:FF:FF:FF.

13.9 RPR Real time Monitor

RPR real time monitor is responsible for traffic monitoring of Client and Span as well as the fault monitoring of Span.

Span refers to the link between two adjacent RPR nodes. Span traffic refers to the traffic between two adjacent RPR nodes. Client traffic refers to the traffic received or sent by the RPR node, and forwarded packets are not included.

- Client Monitor: monitors the Client traffic of the specified RPR interface;
- Span Monitor: monitors the west or east Span traffic of the specified RPR interface;
- Span Error Monitor: monitors the faults occurred on the west or east Span of the specified RPR interface.

The following takes Client Monitor as an example to introduce how to use RPR real time monitor.

Double-click the [RPR Management/Client Monitor] node on the function tree, the system pops up the [Client Monitor] dialogue box, and then click <Select Items> to enter the dialogue box shown in Figure 13-8.

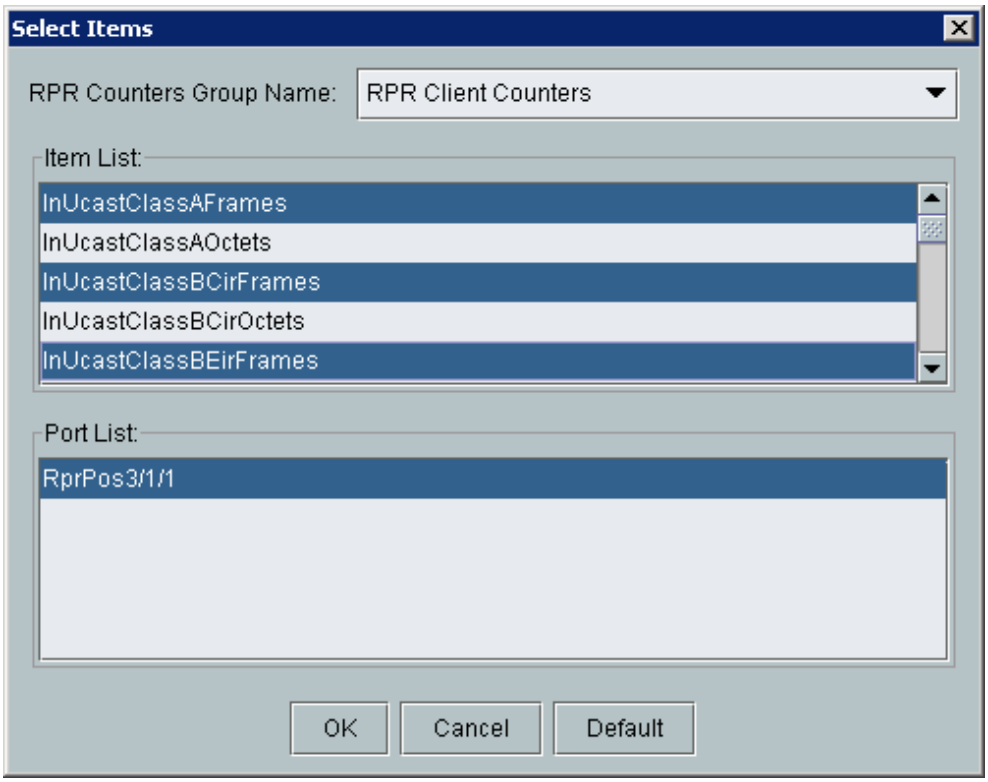


Figure 13-8 Select Items

The above dialogue box can be divided into three parts:

- RPR Counters Group Name;
- Item List: the available items to be selected, vary with different groups;
- Port List: lists all the RPR logical interfaces on the device.

Choose a RPR Counters Group, select one or more items and ports to be monitored, and then click <OK> to enable monitoring. You can view the monitoring result through Histogram or curve line chart as required.

Caution:

Currently, the maximum number of the ports to be monitored is ten and defaults to one.

Chapter 14 Auxiliary Functions

14.1 Address Searching

Address searching is an extended function that can locate the switch port to which a terminal device is connected through its MAC or IP address. This greatly facilitates WAN and MAN management in tracing illegal users or locating fault points. The traditional command line location function requires administrators to have comprehensive network knowledge. On the other hand, location is a time-consuming and heavy work due to large quantity of devices on the network. Once the illegal user is located, its uplink port can be closed or identified.

Double-click on [Auxiliary Tools/Address Searching] node in the function window to open the [Address Searching] dialog box, as shown in Figure 14-1. After entering all necessary information, click <Search>. The system will find the device name, port type and other information corresponding to the address.

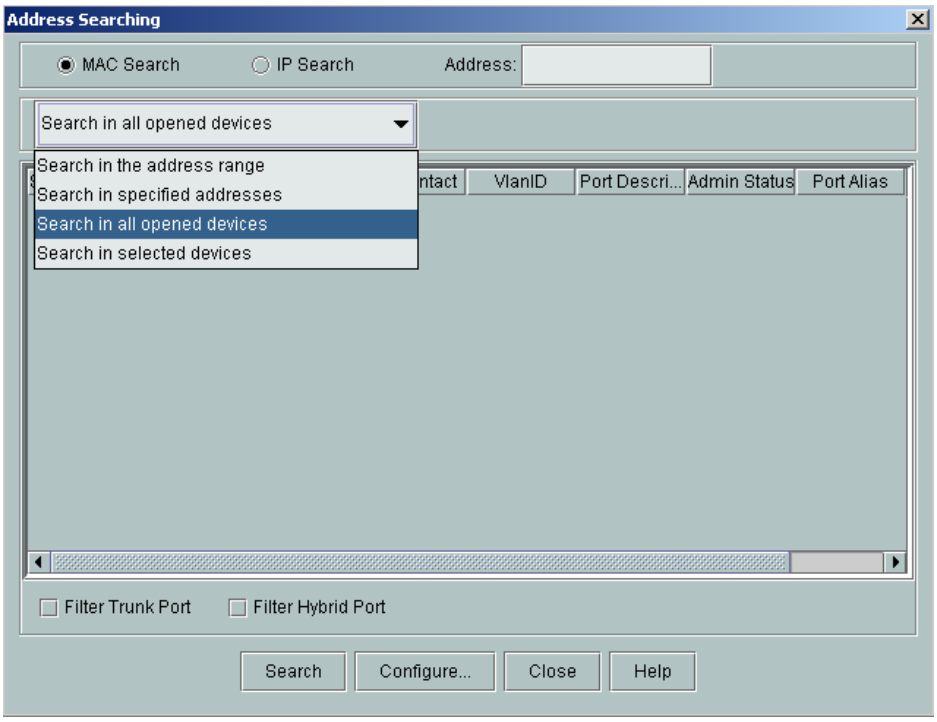


Figure 14-1 Address Searching

The Address Searching function is of two types: searching by MAC address and searching by IP address, which are basically the same. The input information includes:

- Searching mode: Includes MAC search and IP search.

- Address: IP in dotted decimal format or MAC address in hyphen-separated format you are searching for. For example, 10.110.1.1 is a valid IP address and 0005-5d6f-29c2 is a valid MAC address. To search for several addresses at a time, you may enter these addresses separated by comma. Unless indicated otherwise, the IP and MAC addresses appeared elsewhere in this section are in the same format.
- Searching range: The drop-down list box in the second frame provides the following searching ranges for selection:

1) In all opened devices
2) In selected devices
3) In the specified addresses
4) In the address range
5) In cluster

The system masks the five searching ranges according to current user's operating environments, and only lists the available ones. For example, when a multi-device panel is opened but no device is selected, all options except option 5 are available.

When option 3 is selected, the user should further input the IP addresses of these devices separated by comma. When option 4 is selected, the start IP and end IP of the address range are required.

Gateway address: It is required only when searching by IP address, and the gateway must be the direct gateway of the device in search. The user may also specify several gateway addresses separated by comma. Some information on the gateway is required to search for the devices. If no gateway address input, the system will take one of the devices to be searched as the gateway, and try one by one. This will reduce searching efficiency by half or, in large range searching, more. If not knowing the gateway address, you may TraceRoute to the IP and use the penultimate hop address as the gateway address.

Furthermore, the "Filter Trunk Port" and "Filter Hybrid port" options are provided to filter the non-edge (Trunk) or Hybrid ports when the list is large in size. Trunk port is used for network device interconnection, which reflects the status of the path through the terminal device. As is understood, the terminal device is linked to a single edge port at upstream. Subject to the network configurations of the customers, however, the terminal device may be shown to be connected to several edge ports. The reason is that some networks are not configured with multiple VLANs and thus the VLAN Trunk for the sake of simplification, so each network device on the path through the terminal device generates a record as an edge port. In this case, you should recognize the edge port by yourself based on such information listed in the found out port list as switch name, address and administrator.

Caution:

- When searching by IP address, if no gateway address is input and none of the devices within the searching range is a gateway, the searching operation will fail even if the specified IP address is within the range for sure. It is because that only the gateway keeps the mapping relation between the IP addresses and ARP addresses needed for searching. Under rare circumstances, some of the information saved by the administrator during maintenance may be used to find out the device.
- When searching by the address range, you should also note that, as the global SNMP configuration is used for device access, the real SNMP parameter configuration on the device should be consistent with the global configuration, or the searching will fail. In addition, gateway access uses global configuration as well.

The searching results are displayed in a list, as shown in Figure 14-2. The first field is searched address that is used to differentiate several searched addresses from one another. For the searching by a single address, the contents of this field of different records are the same. The subsequent fields are device name, device location, device administrator, VLAN ID, port description, port administrative status, port alias and port VLAN mode respectively.

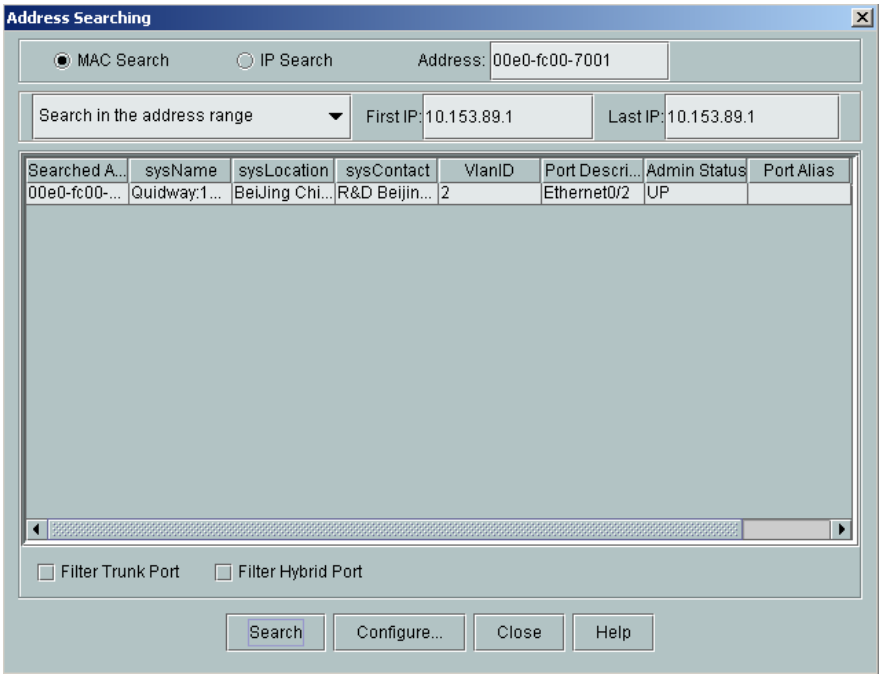


Figure 14-2 Address searching results

You may quickly configure the searched port, such as changing port status (Up/Down) and adding an identifier (alias) to the port, as shown in Figure 14-3.

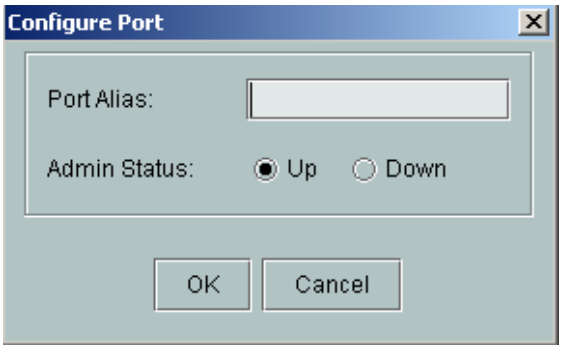


Figure 14-3 Configuring a port

14.2 Port Loopback Test

The loopback test function for port is supported. The operation procedure is as follows: After the Quidview Device Manager starts, select [Device/Open Device…] menu item or click the button to open the panel view of a certain Ethernet Switch. Then select [Auxiliary Tools/Loopback Testing] node from the function window to open the [Port Loopback Test] dialog box, as shown in Figure 14-4. Here select the port to be tested and the test type, and click <Test> to perform the loopback test on the port.

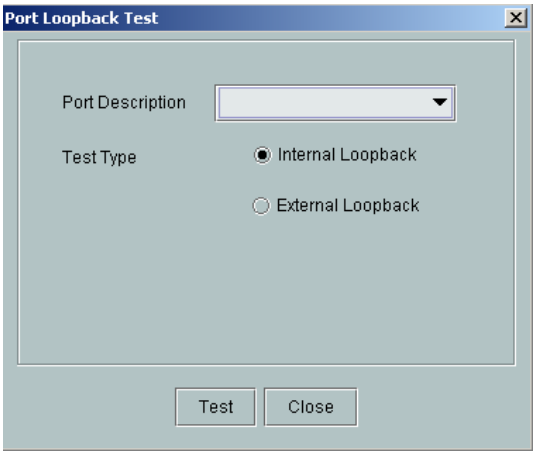


Figure 14-4 Port Loopback Test

Table of Contents

Appendix A Abbreviations A-1

Appendix B FAQ B-1

Appendix C Quidview License Application Procedure C-1

Appendix A Abbreviations

ACL	Access Control List
ADM	Add Drop Multiplexer
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
CIST	Common and Internal Spanning Tree
CST	Common Spanning Tree
DTMF	Dual Tone Multi Frequency
DWDM	Dense Wave Division Multiplexer
FCS	Frame Check Sequences
FXO	Foreign eXchange Office
FXS	Foreign eXchange Station
GARP	Generic Attribute Registration Protocol
GK	GateKeeper
GMRP	GARP Multicast Registration Protocol
GSR	Gigabit Switch Router
GVRP	GARP VLAN Registration Protocol
GW	GateWay
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
LACP	Link Aggregation Control Protocol
LOF	Loss of Frame
LOP	Loss of Pointer
LOS	Loss of Signal
MAC	Medium Access Control
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
OSPF	Open Shortest Path First
PAIS	Path Alarm Indication Signal

POS	Packet Over SDH
POTS	Plain Old Telephone Service
PQ	Strict-Priority Queue
PRDI	Path Remote Defect Indication
PSLM	Path Signal Label Mismatch
PUNEQ	Path Unequipped
QoS	Quality of Service
RAS	Registration, Admission, Status Protocol
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RPR	Resilient Packet Ring
RSTP	Rapid Spanning Tree Protocol
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPE	Synchronous Payload Envelope
STP	Spanning Tree Protocol
TDM	Time Division Multiplexing
VC	Virtual Channel
VDSL	Very high speed Digital Subscriber Line
VLAN	Virtual LAN
VoIP	Voice over IP
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
WRR	Weighted Round Robin

Appendix B FAQ

I. Why did I fail in connecting the host through [Tools/ Telnet…] menu operation?

Please check whether the telnet function has been enabled on the host. You cannot create a telnet connection from a network management station to the host, unless the telnet service is enabled on the latter.

II. Why did I fail in executing the "Telnet" command by selecting [Tools/Telnet…] on a Sun or HP workstation?

To run the "Telnet" command on a Sun or HP workstation, you may need to execute the "/usr/dt/bin/detterm" command first. The "detterm" command, however, is not involved in the environment variables by default, so you should set it to the environment variables or run it manually before running the "Telnet" command.

III. Why did I sometimes fail in creating a VLAN routing interface, prompted not supported by the switch?

VLAN configuration management is a software platform, which supports L2/L3 switches. For a L2 switch, you cannot create a routing interface for a VLAN except the default VLAN.

IV. Why did I fail in opening the device under management in Quidview?

First, check the connectivity of the network with the "Ping" command. If you can ping the device successfully, but still cannot open it in Quidview, do the following to check whether the SNMP community names are correct:

1) Run the following command to telnet to the device under management:

```
Telnet 10.110.99.82
```

2) Execute the following commands in system view to check the SNMP community names of the device:

```
[S3526E] display snmp community read
[S3526E] display snmp community write
```

3) In the "Protocol parameters" dialog box of Quidview, configure the default read-only and read-write community names of the system to the same as those of the device, and click <OK> button.
4) Click <Open> button on the toolbar once again, type the IP address of the device under management in the popup dialog box, and click <OK> button. Then you will be able to open the device.

V. What are the limitations of various types of devices to creation of port aggregation?

The number of port aggregation groups and the maximum number of ports contained in each group vary on different devices in H3C series Ethernet Switches. See Table 6-1 for more detail.

VI. What should be noticed in device configuration?

Note that some configurations conflict with one another, that is, if one is enabled the other must be disabled. For example:

1) IGMP Snooping and GMRP
2) GVRP and Isolate-VLAN
3) Isolate-VLAN and VLAN Trunk

VII. Why did I fail in browsing the up-to-date logging information by opening the "Log" tabbed page in RMON management?

The log browsing function does not support auto refreshing. Click <Refresh> button, and you will see the latest logging information.

VIII. Why was some topology nodes found not being connected with any other nodes on the topology map of a newly created cluster?

Certain switch on the map may be a member of another cluster that has been deleted. Due to communication fault or other problems, the switch's attribute as a member was not modified accordingly. To clear this problem, telnet to the device and execute the following commands in system view:

```
[S3526E] undo cluster enable
[S3526E] cluster enable
```

The first command cancels the membership attribute, and the second command enables the attribute of the device once again.

IX. After a candidate switch was successfully added to a cluster, its icon changed to the member's icon but immediately changed back to the candate's icon. Why?

A password may have been configured on the device. To clear the problem, telnet to the device and run the following command in system view to remove the password:

```
[S3526E] undo super password level 3
```

Thus you will be able to add the device to the cluster.

X. Why was there no interface available while adding a RMON alarm item?

RMON alarm group is correlated to statistics group. Before you can add an alarm item, you must add a related statistics item to the statistics group for the interface.

XI. Why was timeout prompt always received while querying a device?

First, use the "ping" command to check the connectivity of the network. If the managed device is reachable but cannot be opened in the Quidview, please increase the TimeOut time in SNMP Parameter Configuration dialog or check whether the SNMP community names are correct. See question 4 for detailed operation.

XII. What is SNMP?

SNMP is short for Simple Network Management Protocol.

XIII. How many versions of SNMP exist?

SNMPv1 - a widely used standard

SNMPv2p - party-based, obsolete now

SNMPv2c - community-based, in wide use

SNMPv2u - user-based, never in use

SNMPv3 with USM - the latest SNMP standard

XIV. Which version does H3C data communication products support?

SNMPv1, SNMPv2c, and SNMPv3.

XV. The switch and network operated normally. SNMP version, community names (users) and related views' information were properly configured. Why did I fail in connecting the NMS?

Check whether you are excluded outside the firewall.

Do as follows: Run the "display current-configuration" command to browse the configuration or execute such command as "display snmp-agent community/display snmp-agent group" or "display snmp-agent usm-user" to check whether the community name (user) in use or the group it belongs has an ACL in effective, which denies your IP address.

XVI. When I trap a message through trap tool, sometimes there a “hello” message ahead, which travels to the same port as the trap message. Why?

Generally, that happens to the linkdown/linkup and coldstart types of traps because the interface might be down when sending these types of traps. In order to make sure that the Network Management can receive the message, a “hello” string is deployed to send to the specified trap port ahead of trap. This is not a bug.

XVII. Why was timeout always encountered on certain node when I performed the "walk" operation on a device through MIBBrowser?

Except in some special cases, there are several blank tables under the node, when you can change the timeout value of the system to solve the problem.

XVIII. Why did I fail in browsing the preconfigured SNMP commands' information with the "display" command?

You may simply run the "display snmp-agent statistics" command to check whether SNMP Server is disabled. If the system prompts "SNMP Agent disabled", SNMP Server must have been disabled, when you may use the "snmp-agent" command to enable it.

XIX. The MIBBrowser could receive alarms from the router only when the SNMP Version of the switch is configured as v1, instead of v2c (when the MIBBrowser is also configured as v2c). Meanwhile I failed in detecting the alarm packets from the router with NETXRAY in the latter situation. Why?

You should use the following command to configure the host of v2c:

```
snmp-agent target-host Trap address udp-domain x.x.x.x params securityname string v2c
```

XX. How to send a Trap?

First, use the following command to specify the destination host of Trap packets:

```
snmp-agent target-host trap address { udp-domain X.X.X.X [ udp-port port-number ] }  params securityname name-string [ v3 [ authentication | privacy ] | v2c | v1 ]
```

For example:

```
[H3C]snmp-agent target-host trap address udp-domain 10.110.34.73 params securityname public v2c
```

Then use the following command to specify the type of trap to be sent, that is, enable trap function:

```
snmp-agent trap enable [notification-type] [notification-option]
```

For example:

```
[H3C]snmp-agent trap enable standard linkdown
```

To send Trap packets in SNMPv3 format, you should use the "snmp-agent target-host" command to specify the name-string, and configure a v3 user named following the name-string. The v3 user must belong to a specific group with proper view accessing rights.

XXI. Why could the system send SNMPv1 Trap packets only not SNMPv2c Trap packets?

First, check whether SNMPv2c has been enabled. If enabled, check whether the Trap host of v2c has been configured.

XXII. Why the Device Manager cannnot display or configure the voice ports on VG devices?

Currently, the VG devices do not support the related MIB, therefore, the Device Manager could not perform the above operations.

XXIII. Why the DM does not display the changed administrative state of the interface?

Because it takes a period of time to synchronize the information to the MIB. To view the latest state information, wait for a period and refresh the GUI.

Appendix C Quidview License Application Procedure

The Quidview adopts license authorization approach to limit its use. The license can restrict the resident host of Quidview and the number of managed devices. You can get 25 licenses by default when you purchase the Quidview. You just need to purchase expansion license if you have more network devices.

Note:

- If the network adapter on host is replaced, it would be required to gather machine information and apply for license again.
- Single license authorization is only available for one network management solution. For instance, a 200 node license cannot apply to 100 nodes separately, if otherwise, two 100-node licenses should be purchased.

The Quidview is delivered in packaged CDs, with license paper document attached. The installation disk contains Quidview software and a serial number for 90-day free trial.

You can apply for additional licenses in this procedure:

Step 1: The user gets the installation disk.

Step 2: Install the software and it will generate the HostID.dat file which is stored under the installation directory. Or, from [Start/Program/Quidview/Registration] menu, select ‘Generate host ID file’ to regenerate HostID.dat file. Note that the directory for storing the file is required.

Step 3: The user emails the HostID.dat file to license@h3c.com (user information should be contained in the email subject).

Note:

By the way, since the license@h3c.com cannot reply to some types of public mail boxes, you'd better send the HostID.dat file to the local engineer, who can give prompt reply.

If license needs reapplying due to network adapter replacement, expansion application, etc. the original license.dat authorization file and newly gathered HostID.dat file should be sent back.

Step 4: H3C license center generates a license.dat file according to HostID.dat file and serial number.

Step 5: The license center emails the license.dat file to the user.

Step 6: The user registers the file in this way: Run [Start/Program/Quidview/Registration], choose the Register with license file item in the interface, get the right license file and click <Register> button.